УНИВЕРСИТЕТ ИТМО

А.А. Воробьева, В.М. Коржук

СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ВЕДУЩИХ ЗАРУБЕЖНЫХ СТРАНАХ

Часть 2

Учебно-методическое пособие

Санкт-Петербург
2019

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

А.А. Воробьева, В.М. Коржук

СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ВЕДУЩИХ ЗАРУБЕЖНЫХ СТРАНАХ

Часть 2

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

РЕКОМЕНДОВАНО К ИСПОЛЬЗОВАНИЮ В УНИВЕРСИТЕТЕ ИТМО
по направлению подготовки 10.03.01 Информационная безопасность
в качестве учебно-методического пособия для реализации основных
профессиональных образовательных программ высшего образования
бакалавриата

УНИВЕРСИТЕТ ИТМО

Санкт-Петербург
2019

Воробьева А.А., Коржук В.М. **Системы защиты информации в ведущих зарубежных странах. Часть 2.** Учебно-методическое пособие.– СПб: Университет ИТМО, 2019.– 32 с.

Рецензенты: к.т.н. Созинова Е.Н., доцент факультета безопасности информационных технологий Университета ИТМО

Учебное пособие разработано для методической помощи бакалаврам, обучающимся по направлению подготовки 10.03.01 – «Информационная безопасность».

В пособии рассмотрены вопросы правового обеспечения информационный безопасности в зарубежных странах. Предложены практические задания для изучения законодательства зарубежных стран в области компьютерных преступлений, а также задания для изучения лучших практик по разработке стратегий информационной и кибербезопасности.
Представлен вспомогательный теоретический материал по определению понятий «киберпреступление», «компьютерное мошенничество», «форензика», описаны особенности классификации секретной информации в ведущих зарубежных странах. Сформулированы рекомендации по изучению и анализу стратегических и нормативно-правовых документов, разработанных и действующих в ведущих зарубежных странах, практики зарубежных стран по раскрытию киберпреступлений, механизмов составления национальной стратегии кибербезопасности на примере зарубежных стран. Предложены ситуационные задания, направленные на развитие навыков поиска дополнительной информации и анализа инцидента информационной безопасности и критического мышления, навыков работы с международными и локальными регулирующими документами.
Учебное пособие может быть рекомендовано бакалаврам, осуществляющих подготовку по направлению «Информационная безопасность», руководителям и специалистам информационных, юридических служб, IT подразделений и подразделений по технической защите информации.

УНИВЕРСИТЕТ ИТМО

Университет ИТМО – ведущий вуз России в области информационных и фотонных технологий, один из немногих российских вузов, получивших в 2009 году статус национального исследовательского университета. С 2013 года Университет ИТМО – участник программы повышения конкурентоспособности российских университетов среди ведущих мировых научно-образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО – становление исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Компьютерные преступления и задачи обеспечения информационной и компьютерной безопасности существуют уже давно, ориентировочно с середины 1960-х годов. Несмотря на долгую историю компьютерной преступности, и сегодня не существует единой устоявшейся терминологии в данной области. Существенно разнится перечень деяний, относимых к компьютерным преступлениям, а также меры ответственности за совершение подобных деяний. Подобного рода расхождения в законодательствах различных стран ведут к возникновению так называемых безопасных убежищ для преступников и также препятствуют сбору доказательств во всех странах мира.

Международная информационная безопасность – состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве (РФ)[1].

Согласно документам ООН, международная информационная безопасность – это защищенность глобальной информационной системы от так называемой «триады угроз» – террористических, преступных и военно-политических. Под военно-политическими угрозами современные исследователи понимают кибер- или информационные войны и информационное противоборство (подробно рассмотрены в первой части пособия).

Информационная безопасность государства – состояние сохранности информационных ресурсов государства и защищённости законных прав личности и общества в информационной сфере[2].

Информационная безопасность – состояние защищенности информационной среды, обеспечивающее ее формирование, применение и развитие в интересах граждан, организаций, государства[3];

Информационная безопасность информационной системы – это процесс обеспечения конфиденциальности, целостности и доступности информации[4].

Основной организацией, координирующей усилия государств по осуществлению мероприятий в области обеспечения информационной безопасности и борьбы с преступлениями в сфере информационных технологий, является ООН. Именно в рамках ООН разрабатываются и принимаются акты и иные документы, отражающие взгляды большинства стран мира на вопросы безопасности, в частности, на существующие

[1] Конвенция об обеспечении международной информационной безопасности (концепция) URL: http://www.scrf.gov.ru/documents/6/ 12.html (дата обращения: 25.07.2019).

[2] Пилипенко В. Ф. Безопасность: теория, парадигма, концепция, культура. Словарь-справочник //М.: ПЕР СЭ-Пресс. – 2005.

[3] Федеральный закон от 04.07.1996 N 85-ФЗ (ред. от 29.06.2004) "Об участии в международном информационном обмене".

[4] ГОСТ Р ИСО/МЭК. 17799-. 2005. Информационная технология. ПРАКТИЧЕСКИЕ ПРАВИЛА УПРАВЛЕНИЯ. ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ.

проблемы и вызовы. Такие документы не накладывают юридические обязательства на государства. Они могут содержать некоторые рекомендации и служить основой или моделью для разработки единообразных национальных законодательств.

В Российской Федерации к триаде угроз политики добавляют опасность вмешательства во внутренние дела суверенного государства посредством информационно-коммуникационных технологий (ИКТ), нарушение общественной стабильности и разжигание межэтнической, межнациональной розни.

На сегодняшний день основной проблемой в данной области является отсутствие единой устоявшейся терминологии. Если Россия подразумевает под международной ИБ совокупность безопасности информационных и коммуникационных систем и сетей (то есть защиту технической направленности) и безопасности политических, идеологических и правовых аспектов (манипулирование информацией, пропаганда посредством глобальных информационных сетей, информационное воздействие), то страны Запада и США стремятся к обеспечению кибербезопасности, понимая под этим понятием защиту информации в киберпространстве (ЗИ). Общим является стремление противодействовать терроризму и международной информационной преступности.

Россия, как и Китай, придерживается позиции о необходимости полной демилитаризации информационного пространства. По мнению РФ, гонка вооружений в информационной сфере способна расшатать сложившиеся договоренности о разоружении и международной безопасности.

США, как и ЕС, придерживаются позиции, согласно которой ключевыми угрозами кибербезопасности являются кибертерроризм и киберпреступность, а вопросы межгосударственного противоборства в киберпространстве следует регулировать в рамках международного гуманитарного права [6].

В законодательствах различных стран отношение и перечень деяний, относимых к компьютерным преступлениям, существенно различается. Разнятся также и используемые термины, наиболее часто используются термины: «киберпреступления», «компьютерные преступления» или «преступления в сфере высоких технологий».

Основное отличие понятий «компьютерные преступления» и «информационная безопасность» от «киберпреступлений» и «кибербезопасности» состоит в том, что под первыми понятиями подразумевают несколько более локальные проблемы и задачи, существующие в большей степени для конкретных организаций. Кибербезопасность несколько более широкое понятие, под которым понимают обеспечение безопасности всего общества.

Определения киберпреступности преимущественно зависят от цели использования этого термина. Под это понятие попадает ограниченный круг деяний, направленных против конфиденциальности, целостности и доступности компьютерных данных или систем. Такие виды преступлений, как правило, четко прописаны в законодательствах. Но часть действий, которые можно отнести к киберпреступности не всегда имеет правовое определение, соответственно и преследование за подобные действия часто удается избежать. В качестве примеров можно привести такие деяния как использование компьютера в целях извлечения личной или финансовой прибыли или причинения личного или финансового вреда, в том числе формы преступлений, связанных с использованием персональных данных, и деяния, связанные с содержанием компьютерных данных[5].

Под *компьютерным преступлением* или *киберпреступлением* понимают следующее:

1. любого рода преступления, связанные с компьютерной техникой, которые при этом противоречат праву (Седаков С.Ю.);

2. действия, совершаемые с целью получения и использования информации в компьютерной сфере, при этом информация может являться как предметом, так и средством совершения преступления [9];

3. незаконное и неразрешенное поведение, которое тесно соприкасается с обработкой и передачей данных (Бекряшев А.К.);

4. опасные действия, предусмотренные уголовным законом, в которых информация ЭВМ является объектом преступления (Вехов В.Б.);

5. нарушения личных интересов и чужих прав в отношении любого вида автоматизированных систем обработки данных, которые намеренно совершаются во вред правам и интересам людей, общества и государства (Анин Б.).

При этом существует два взгляда на компьютерные преступления: первый характеризуется тем, что информация может быть и объектом, и субъектом преступления, а второй – что преступление является действием в системе или сети автоматизированной обработки информации, направленным на нарушения существующего законодательства.

Наука, которая занимается раскрытием инцидентов и преступлений, связанных с компьютерной информацией, и исследованием цифровых доказательств, методов поиска, получения, анализа и закрепления таких

[5] Всестороннее исследование проблемы киберпреступности // УНП ООН Управление Организации Объединенных Наций по наркотикам и преступности. 2013. URL: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf (дата обращения: 12.10.2019).

доказательств, называется компьютерной криминалистикой или *форензикой*, Задачами форензики являются:

1. построение общей концепции атаки (особенности реализации);
2. разработка сценария взлома;
3. восстановление хронологической последовательности этапов атаки;
4. сбор и анализ следов атак (улик, так называемых артефактов);
5. разработка рекомендаций и превентивных защитных мер для предотвращения повторения атаки;
6. формирование экспертного заключения о результатах экспертизы.

В данном учебно-методическом пособии сделан акцент на изучении ряда национальных и международных правовых документов зарубежных стран, затрагивающих вопросы противодействия и расследования компьютерных преступлений и обеспечения национальной информационной безопасности. В процессе выполнения практических заданий студенты изучают основные регламентирующие документы стран Европейского Союза и Соединенных Штатов Америки в области правового обеспечения защиты информации; проводят сравнительный анализ подходов и практик противодействия и расследования киберпреступлений в Российской Федерации и в ведущих зарубежных странах; учатся применять критическое мышление к анализу и интерпретации существующих положений в области национальных стратегий компьютерной безопасности с точки зрения ведущих зарубежных стран, таких как Великобритания, Соединенные Штаты Америки, Китай, Япония и др.

Национальная стратегия компьютерной безопасности (кибербезопасности) является составной частью стратегии национальной безопасности. Несмотря на разногласия в определении понятия «кибербезопасность», существует перечень близких по содержанию принципов [21]:

1. планирование и определение необходимых политик и регулирующих механизмов, четкое обозначение ролей, прав и ответственности для частного и государственного сектора (например, новая законодательная база для борьбы с киберпреступностью, обязательное информирование об инцидентах безопасности, базовые меры обеспечения безопасности и руководства к действию, новые нормы материально-технического обеспечения);

2. определение целей и способов развития государственных возможностей и необходимой законодательной базы для вступления в международную борьбу с киберпреступностью;

3. определение критических информационных инфраструктур, в том числе основных активов, сервисов и взаимозависимостей;

4. повышение готовности, уменьшение времени реакции на инциденты, разработка плана восстановления после сбоев и механизмов защиты для критических информационных инфраструктур (например, национальный план действий в особой обстановке, порядок поведения в киберпространстве, ситуационная осведомленность);

5. разработка системного и интегрированного подхода к государственному управлению рисками (например, доверенный обмен информацией и государственные реестры рисков);

6. доказательство необходимости новой программы образования, делающей упор на обучение IT-специалистов и профессионалов в области кибербезопасности.

7. международное сотрудничество как со странами-членами Евросоюза, так и со странами, не входящими в Евросоюз (например, принятие международных соглашений).

Для выполнения работ, представленных в пособии, необходимо изучение теоретического материала по тематикам программы дисциплины, в том числе лекционных материалов и материалов для самостоятельного изучения. Дисциплина включает два цикла практических работ, направленных на приобретение практических умений и навыков.

Вторая часть учебно-методического пособия содержит цикл из четырех работ, направленных на изучение правового обеспечения ИБ и кибербезопасности и методов борьбы с компьютерными преступлениями в ведущих зарубежных странах, практики зарубежных стран по расследованию и уголовному преследованию компьютерных преступлений, а также анализу и разработке проекта национальной стратегии компьютерной безопасности.

В соответствии с описанными в пособии рекомендациями, студенты выполняют практические работы в малых группах (командах) по 3–4 человека. Процесс работы представляет собой совместную разработку решений и очную защиту отчетов. Работа ведется в соответствии с вариантом задания и направлена на решение общей задачи путем творческого сложения результатов индивидуальной работы членов команды с делением полномочий и ответственности. В результате работы каждая команда совместно представляет публичный доклад. После доклада выступающие отвечают на вопросы преподавателя и студентов-слушателей.

Часть занятий представляют собой занятия типа «case-study» – анализ и разбор реальных проблемных ситуаций, имевших место в соответствующей области профессиональной деятельности, и поиск вариантов лучших решений. Для выполнения заданий такого типа необходимо заранее (до начала занятия) ознакомиться с методическими

указаниями, рекомендованными источниками литературы по данной теме. Кроме этого, необходимо качественно интерпретировать итоги выполнения практической работы, а также подготовиться к ответу на контрольные вопросы. Во время работы рекомендуется активно участвовать в обсуждении и формировании решения для поставленного задания, по итогам проанализировать процесс работы и полученные результаты и выявить ошибки.

Занятия типа «семинар» проводятся на основе разработанного плана, по вопросам которого готовится вся учебная группа. Группа докладчиков совместно готовит реферат, презентацию и доклад по теме семинара. После доклада участники семинара задают вопросы, на которые отвечает выступавшая группа докладчиков.

Самостоятельная работа студентов (СРС) по дисциплине играет важную роль в ходе всего процесса обучения с целью усвоения материала дисциплины. В ходе СРС студенты изучают теоретические материалы, основную и дополнительную литературу, готовят и оформляют реферат, готовятся к докладу и презентации.

Практическая работа № 1. Правовое обеспечение информационной безопасности и борьба с компьютерными преступлениями в ведущих зарубежных странах

Форма проведения

семинар.

Цель работы

изучить правовые аспекты защиты информации в зарубежных странах.

Задачи

- изучить правовые аспекты защиты информации в США, Великобритании, Германии, Франции, Японии, КНР;
- изучить вопросы международного сотрудничества по обеспечению информационной безопасности и по борьбе с киберпреступлениями.

Описание

Методы исследования: теоретическое исследование (поиск, сбор, группировка и анализ информации по теме работы).

Ход выполнения

Задание для докладчиков:

1. Изучить государственные органы обеспечения кибербезопасности в указанных странах.

2. Изучить классификацию секретной информации в указанных странах.

3. Изучить законодательства в области информационной безопасности и компьютерных преступлений в указанных странах. В том числе изучить государственные стратегии кибербезопасности в странах ЕС и США.

4. Изучить зарубежный опыт защиты государственной тайны, системы классификации секретной информации, особенности допуска к секретной информации, порядок засекречивания и рассекречивания информации в зарубежных странах.

Вопросы для обсуждения на семинаре

В начале занятия дайте ответы на следующие вопросы:

1. Были ли когда-то компьютеры использованы против вас или ваших знакомых (в том числе украденные аккаунты, электронные почты и пр.)? Понесли ли преступники наказание за это? Как вам кажется, достаточным

(недостаточным) ли было это наказание? Если преступникам удалось избежать наказания, как вам кажется, по каким причинам это произошло?

2. Допустим, вам стало известно, что совершенные злоумышленником действия являются преступлением. Что вы бы могли предпринять?

После доклада необходимо разбиться на группы и выполнить следующие задания:

1. Произвести анализ подходов к правовому обеспечению информационной безопасности и между указанными странами;

2. Сравнить существующие подходы к правовому обеспечению информационной безопасности указанных стран и РФ;

3. Определить возможности использования зарубежного опыта для улучшения защиты информации и борьбы с компьютерными преступлениями в России.

Содержание реферата, доклада, презентации

1. Государственные органы обеспечения кибербезопасности в указанных странах.

2. Законодательство в области информационной безопасности и компьютерных преступлений в указанных странах. В том числе изучить государственные стратегии кибербезопасности в странах ЕС и США.

3. Сравнительный анализ подходов к правовому обеспечению информационной безопасности между указанными странами, также сравнить с РФ.

4. Подходы к защите государственной тайны в зарубежных странах, различия в системе классификации секретной информации, отличительные особенности допуска к секретной информации, особенности засекречивания и рассекречивания информации. Наказание за нарушение прав допуска, за разглашение и прочие преступления, связанные с государственной тайной.

Краткая теоретическая справка

В США в настоящее время действует классификация секретной информации, установленная указом президента Барака Обамы от 2009 года. При оценке степени секретности информации в США используется термин *information sensitivity* (рус. ~ *информационная чувствительность*), не имеющий точного аналога в русском языке. Sensitivity по смыслу является более близкой к понятию «риск ИБ» и обозначает уровень ущерба, который может нанести национальной безопасности США раскрытие данной информации. В США есть три уровня секретности информации, по мере возрастания: confidential – «секретно», secret – «совершенно секретно» и top secret – «совершенно секретно, особой важности». Необходимо отметить,

что в США отсутствует единый закон о государственной тайне. Информация открытого доступа имеет название unclassified information.

Политика защиты правительственной секретной информации в Великобритании в настоящее время определяется руководством Security Policy Framework в редакции от 2013 года. Классификация секретной информации описывается пятью уровнями: top secret – «совершенно секретно, особой важности», secret – «совершенно секретно», confidential – «секретно», restricted – «ограниченный доступ», protect – «защищенная информация», unclassified – открытая информация. Содержание SPF разработано частично Управлением безопасности аппарата Кабинета министров Великобритании, частично – центром правительственной связи (главным органом Великобритании в сфере криптографии и защиты правительственной информации).

В Китайской Народной Республике с 1989 года существует «Закон об охране государственной тайны». Этот закон предусматривает три категории секретной информации: «совершенно секретно» – определяется как «жизненно важные государственные секреты, раскрытие которых может причинить очень серьёзный ущерб государственной безопасности и национальным интересам»; «высокая секретность» – определяется как «важные государственные тайны, раскрытие которых может нанести серьёзный ущерб государственной безопасности и национальным интересам»; «секретно» – определяется как «обычные государственные тайны, разглашение которой может нанести вред государственной безопасности и национальным интересам». Наряду с государственным органом по защите государственных тайн, в КНР также существует аналогичный партийный орган – «Центральный комитет по защите государственной тайны», подчинённый Центральному комитету Коммунистической партии Китая.

Для обмена конфиденциальной информацией между странами «большой семерки» был разработан специальный протокол Traffic Light. Этот протокол в настоящее время принят в качестве основы для защищенного обмена информацией более чем в 30 странах. Протокол предусматривает четыре уровня секретности информации — «красный», «жёлтый», «зелёный» и «белый».

Рекомендованная литература

[1, 6, 8, 13, 22–27]

Практическая работа № 2. Практика зарубежных стран по расследованию и уголовному преследованию компьютерных преступлений

Форма проведения

case study – анализ реальных проблемных ситуаций, имевших место в соответствующей области профессиональной деятельности, и поиск вариантов лучших решений.

Цель работы

изучить практику расследования и уголовного преследования за компьютерные преступления путем анализа реальных инцидентов прошлых лет.

Описание

Работа выполняется в группах по 3–4 человека, сформированных ранее. В ходе выполнения необходимо опираться на следующие документы:

1. Конвенция Совета Европы о киберпреступности.
2. Уголовный кодекс соответствующих стран.

Ход выполнения

1. Выбрать по одному компьютерному преступлению для первой и второй группы. Рекомендуется выбрать случаи, затрагивающие международные отношения (например, аресты российских хакеров в США).

Группа 1:

a. Преступления против компьютерных данных и систем.

b. Компьютерное мошенничество и фальсификация.

Группа 2:

a. Преступления, связанные с контентом (детская порнография, ксенофобия, расизм и пр.).

b. Преступления, связанные с правом на интеллектуальную собственность.

2. Для каждого преступления определить:
   a. Цель и мотив преступления.
   b. Субъект (государство, коммерческие организации, частное лицо) и объект атаки.
   c. Механизм совершения.
   d. Причиненный ущерб.

e. Изучить предъявленные доказательства, в том числе электронные.

f. Под какие статьи попадает данное преступление или по каким статьям было предъявлено обвинение? Привести максимальное и минимальную ответственность за совершение.

g. Какое наказание было применено к злоумышленнику?

h. Определить эффективность принятых мер.

i. Подготовить презентацию и доклад.

Форма отчета

Защита работы проходит в форме представления доклада и презентации. Необходимо подготовить доклад и презентацию на каждый рассмотренный случай. Время одного доклада по одному кейсу 3–4 минуты, дополнительно дается 1–2 минуты на вопросы.

Содержание доклада и презентации

Каждая презентация и доклад должны обязательно содержать следующее:

1. Цель и мотив преступления.
2. Субъект (государство, коммерческие организации, частное лицо) и объект атаки.
3. Механизм совершения.
4. Причиненный ущерб.
5. Предъявленные обвинением доказательства.
6. Статьи законодательства в области компьютерных преступлений.
7. Наказание преступника.
8. Оценка и обоснование эффективности принятых мер.

Варианты

Необходимо самостоятельно произвести подбор кейсов (ситуаций) и предварительно согласовать его с преподавателем.

Краткая теоретическая справка

Необходимо отметить, что, в соответствии с конвенцией о киберпреступности совета Европы, преступления против конфиденциальности, целостности и доступности компьютерных данных и систем, преступления, связанные с контентом, и преступления, связанные с правами собственности, сфокусированы на объекте юридической защиты, а преступления, связанные с компьютерами, сфокусированы на методе.

Под преступлениями против компьютерных данных и систем понимается несанкционированный доступ к информации (хакерство, взлом), неправомерный перехват информации, воздействие на данные (искажение), воздействие на функционирование системы и противозаконное использование устройств.

Под компьютерным мошенничеством понимается завладение чужим имуществом путем обмана, злоупотребления доверием, присвоения, растраты, а также причинение имущественного ущерба путем обмана или злоупотребления доверием с использованием средств компьютерной техники. В перечень действий, относимых к мошенничеству, входит любой ввод, изменение, стирание или подавление компьютерных данных и любое вмешательство в функционирование компьютерной системы, подлоги с использованием компьютера, кража идентичности, неправильное использование устройств.

Рекомендованная литература

[2–4, 7, 9, 11, 14, 16, 17, 21, 28–29]

Практическая работа № 3. Правовые аспекты обеспечения кибербезопасности в зарубежных странах

Форма проведения

case study – анализ реальных проблемных ситуаций, имевших место в соответствующей области профессиональной деятельности, и поиск вариантов лучших решений.

Цель работы

исследовать правовые аспекты защиты информации в зарубежных странах.

Задачи

- изучить вопросы международного сотрудничества по борьбе с киберпреступлениями;
- изучить практику применения законодательства для преследования основных типов компьютерных преступлений.

Описание

Работа выполняется в группах по 3–4 человека, сформированных ранее. В ходе выполнения необходимо опираться на следующие документы:

1. Конвенция Совета Европы о киберпреступности.
2. Уголовный кодекс соответствующих стран.

Ход выполнения

Для каждого из сценариев в соответствии с вариантом определите:

1. Тип преступления.
2. Способ совершения преступления.
3. Мотив и круг подозреваемых.
4. Применяемые статьи законодательства зарубежных стран в области компьютерных преступлений (в соответствии с вариантом).
5. Лица, несущие ответственность.

Сценарии

Группа 1

1. Электронная почта или аккаунт в социальной сети жертвы был взломан, после чего жертва получила требования о выплате «выкупа» за возврат доступа к электронной почте, аккаунту.

2. Электронная почта или аккаунт в социальной сети жертвы был взломан, после чего была совершена рассылка сообщений по всем контактам с просьбой о перечислении средств на счет преступников.

3. Электронная почта или аккаунт в социальной сети жертвы был взломан, после чего была совершена рассылка сообщения по всем контактам, содержащего вредоносное вложение (вирус, троян и пр.). В результате компьютеры лиц, получивших сообщение и открывших вложение, были заражены.

4. Электронная почта или аккаунт в социальной сети жертвы был взломан, после чего была совершена рассылка сообщения по всем контактам с порочащим жертву содержанием.

Группа 2

1. Злоумышленники обманным путем похитили средства со счета жертвы с использованием онлайн переводов через интернет-банкинг:

a. переводы на финансирование запрещенных организаций;

b. переводы на счета злоумышленников.

2. Злоумышленники совершили ряд онлайн покупок с использованием банковской карты жертвы, при условии, что карта находится у владельца.

Группа 3

1. От потерпевшей поступила жалоба, что некто создал ее фальшивый профиль в социальной сети и публикует там порочащую ее информацию, сообщения и фотографии. Фальшивый профиль содержит ее настоящие имя/фамилию, контактные данные и фотографии, в результате чего страдает репутация жертвы.

2. Злоумышленник опубликовал персональную информацию жертвы, включая имя, фотографии, номер мобильного телефона и электронную почту на сайте знакомств «для взрослых». В результате жертва получает большое число нежелательных звонков и сообщений.

Группа 4

1. Жертва получила электронное письмо из налоговой службы, содержащее просьбу выслать всю информацию о банковских счетах жертвы. Позже со счетов жертвы были похищены 6000 тыс. у.е.

2. Жертвой было получено электронное сообщение, содержащее информацию, что он / она является победителем лотереи, и просьбу перечислить некоторый депозит, для того чтобы получить возможность участия в розыгрыше призов.

3. Жертва получила электронное письмо из его банка, содержащее просьбу пройти процедур смены пароля к системе Интернет-банкинга. Позже со счетов жертвы были похищены 6000 тыс. у.е.

Группа 5

1. Злоумышленником (внешним или сотрудником компании) были похищены исходные коды ПО, позже проданные конкурирующей компании.

2. Злоумышленником (внешним или сотрудником компании) были похищены исходные коды ПО, позже использованные для создания собственного ПО.

Группа 6

1. Злоумышленником были похищены корпоративные данные (путем взлома или социальной инженерии), позже он требовал выкуп, угрожая разглашением данной информации или передачей ее конкурентам.

2. Недовольным сотрудником компании были похищены корпоративные данные, позже он разместил эту информацию в открытый доступ на ряде Интернет сайтов.

3. Конкурирующей организацией были похищены корпоративные данные (бизнес-планы, базы поставщиков и клиентов, коммерческие предложения) путем взлома или социальной инженерии, позже данные были использованы для получения выгоды.

Группа 7

1. Злоумышленники занимаются продажами пиратского ПО на физических носителях.

2. Злоумышленники занимаются распространением пиратского ПО с использованием электронных ресурсов (сайты, форумы, торренты).

3. Злоумышленники занимаются продажами аудио-контента на физических носителях.

4. Злоумышленники занимаются распространением аудио-контента с использованием электронных ресурсов (сайты, соц. сети, форумы, торренты).

Группа 8

Злоумышленник занимается распространением порнографического контента с использованием собственного веб-сайта и взымает за это плату.

Группа 9

1. Злоумышленник создал/запустил вирус в сеть, атака направлена на все компьютеры под управлением ОС Windows.

2. Компьютеры и сервера некоторой компании оказались заражены новым, ранее не известным вирусом. Похоже, что данный вирус был специально разработан для этой атаки.

Группа 10

1. Злоумышленник взломал сайт некоторой компании и разместил на нем порочащее компанию содержание.

2. Злоумышленник взломал сайт государственной организации и разместил на нем порочащее компанию содержание.

Группа 11

1. Злоумышленниками была создана страница (в соц. сети, на сайте), содержащая информацию, порочащую репутацию вашей компании/товара.

2. Злоумышленниками была создана страница (в соц. сети, на сайте), содержащая информацию негативной направленности против определенной группы лиц (определенного пола/цвета кожи/вероисповедания и пр.)

Группа 12

Рассмотрите следующие вопросы, выступите в роли обвинителей. Сотрудниками спец. служб страны А был задержан некоторый субъект Z. Какие обвинения и по каким статьям ему могут быть предъявлены, какое наказание ему грозит?

1. Субъект рассказывает следующую историю: случайным образом он получил некоторый электронный носитель государственной тайны, принадлежащей стране А, факт содержания данной информации ему известен не был. Далее, просмотрев на собственном компьютере данный носитель информации, он определил секретность содержащихся на нем сведений. При повторном просмотре данного носителя на этом же компьютере он был задержан.

2. Спец. службам доподлинно известно, что Z похитил носитель информации, составляющей государственную тайну, принадлежащую стране А, так как он был задержан в момент совершения похищения, факт нахождения у него данного носителя был зафиксирован.

Форма отчета

Защита работы проходит в форме защиты отчета. На защите должны присутствовать все студенты, выполнявшие работу.

Содержание отчета

1. Описание ситуации (задание).

2. Тип преступления.

3. Способ совершения преступления.

4. Мотив и круг подозреваемых.

5. Применяемые статьи законодательства зарубежных стран в области компьютерных преступлений (в соответствии с вариантом).

6. Лица, несущие ответственность.

7. Использованная литература.

Также отчет должен обязательно включать титульный лист с номером варианта, фамилий и номеров групп студентов, выполнявших работу.

Варианты

Вариант	Сценарии												Страны		
	1	2	3	4	5	6	7	8	9	10	11	12	Европа и ЕС	ШОС и БРИКС	США
1.	1	1	1	1	1	1	4	1	2	1	1	1	Великобритания	КНР	США
2.	2	1	1	1	1	1	3	1	1	2	1	2	Германия	Индия	США
3.	3	1	1	1	2	1	2	1	2	1	2	1	Франция	КНР	США
4.	4	1	1	2	2	2	1	1	1	2	2	2	Нидерланды	Индия	США
5.	1	2	2	2	1	2	4	1	2	1	1	1	Австрия	КНР	США
6.	2	2	2	2	1	2	3	1	1	2	1	2	Финляндия	Индия	США
7.	3	2	2	3	2	3	2	1	2	1	2	1	Швеция	КНР	США
8.	4	2	2	3	2	3	1	1	1	2	2	2	Эстония	Индия	США
9.	1	1	2	3	1	3	4	1	2	1	1	1	Великобритания	КНР	США
10.	2	1	2	1	1	1	3	1	1	2	1	2	Германия	Индия	США
11.	3	1	2	1	2	1	2	1	2	1	2	1	Франция	КНР	США
12.	4	1	2	1	2	1	1	1	1	2	2	2	Нидерланды	Индия	США
13.	1	2	1	1	1	1	4	1	2	1	1	1	Австрия	КНР	США
14.	2	2	1	2	1	2	3	1	1	2	1	2	Финляндия	Индия	США
15.	3	2	1	2	2	2	2	1	2	1	2	1	Швеция	КНР	США
16.	4	2	1	2	2	2	1	1	1	2	2	2	Эстония	Индия	США
17.	1	1	1	3	1	3	4	1	2	1	1	1	Великобритания	КНР	США
18.	2	1	1	3	1	3	3	1	1	2	1	2	Германия	Индия	США
19.	3	1	1	3	2	3	2	1	2	1	2	1	Франция	КНР	США
20.	4	1	1	1	2	1	1	1	1	2	2	2	Нидерланды	Индия	США
21.	1	2	2	1	1	1	4	1	2	1	1	1	Австрия	КНР	США
22.	2	2	2	1	1	1	3	1	1	2	1	2	Финляндия	Индия	США
23.	3	2	2	2	2	2	2	1	2	1	2	1	Швеция	КНР	США
24.	4	2	2	2	2	2	1	1	1	2	2	2	Эстония	Индия	США

Рекомендованная литература

[5, 10, 12, 13, 18, 19, 21, 28–29]

Практическая работа № 4. Разработка национальной стратегии компьютерной безопасности

Форма проведения

case study – анализ реальных проблемных ситуаций, имевших место в соответствующей области профессиональной деятельности, и поиск вариантов лучших решений.

Цель работы

Изучить практику разработки национальных стратегий компьютерной безопасности в зарубежных странах, опираясь на анализ текущей ситуации и регламентирующие и рекомендательные международные документы.

Описание

Тип работы: работа в команде. Работа выполняется в группах по 3–4 человека, сформированных на предыдущих занятиях.

В ходе выполнения необходимо опираться на следующие документы:

1. Конвенция Совета Европы о киберпреступности.
2. Существующие национальные стратегии кибер- или компьютерной безопасности (в соответствии с вариантом).
3. Рекомендации ENISA.

Ход выполнения

Группа студентов выступает в роли экспертной группы по подготовке проекта стратегии национальной кибербезопасности и плана ее внедрения.

Необходимо разработать текст стратегии и дорожную карту для ее реализации, а также подготовить презентацию для представления ее «Министру по безопасности» или другому высокопоставленному лицу, принимающему решения.

1. Предварительно необходимо произвести анализ и оценить текущую ситуацию обеспечения ИБ (кибербезопасности, компьютерной безопасности) на государственном уровне:
    a. Юридические меры. Законодательные и иные национальные документы (стратегии, планы). Насколько они соответствуют текущим вызовам?
    b. Существуют ли государственные стандарты компьютерной безопасности? Как производится сертификация?
    c. Государственные организации по вопросам компьютерной безопасности, в том числе:
        i. Государственные органы, ответственные за компьютерную безопасность.

ii. Группы реагирования на инциденты компьютерной безопасности.

d. Предпринимаемые шаги для улучшения ИБ:
   i. Человеческие ресурсы (повышение осведомленности, обучение, сертификация)
e. Качество международного сотрудничества.

2. Необходимо определить:
   a. основные цели;
   b. основные проблемы и угрозы безопасности государственного масштаба;
   c. концепцию стратегии;
   d. основные задачи предотвращения и снижения угроз;
   e. пути достижения состояния защищенности от выявленных угроз (план реагирования);
   f. основных участников, вовлеченных в процесс реализации стратегии.
3. Необходимо разработать план внедрения стратегии.

Стратегия должна быть разработана с учетом рекомендаций международных организаций (ООН, Совета Европы, ШОС).

Форма отчета

Защита работы проходит в форме представления текста стратегии (3–5 страниц) и плана внедрения (дорожная карта), презентации и доклада. Время доклада 5 минут, дополнительно дается 1–2 минуты на вопросы.

Варианты

1. Великобритания
2. Германия
3. Франция
4. Нидерланды
5. Австрия
6. Финляндия
7. Швеция
8. Эстония
9. Норвегия
10. КНР
11. Индия
12. Бразилия
13. ЮАР
14. Канада
15. Новая Зеландия
16. Испания
17. Израиль
18. Турция
19. Латвия
20. Литва
21. Азербайджан
22. Казахстан

Краткая теоретическая справка

ENISA – European Union Agency for Cybersecurity – Европейское агентство по сетевой и информационной безопасности, образованное в 2004 году под названием European Network and Information Security Agency. Основные задачи ENISA – отражать кибератаки нацеленные на институты Евросоюза, органы государственной власти, а также оказывать помощь

государствам-членам в случае атак и сбоев в принадлежащих им сетях. Также частью обязанностей ENISA является оказание содействия в развитии превентивных мер и средств борьбы с угрозами информационной безопасности. ENISA поддерживает разработку совместных мер реагирования на крупномасштабные трансграничные инциденты и кризисные ситуации в области кибербезопасности и с 2019 года разрабатывает схемы сертификации средства обеспечения кибербезопасности.

Рекомендованная литература

[1, 3, 6, 15, **20, 30**–**41**]

ОПИСАНИЕ ПРОВЕДЕНИЯ СЕМИНАРОВ

Часть практических занятий проводится в виде семинара по теме занятия для систематизации теоретических и фактических знаний в определенном контексте (подготовка и презентация материала по определенной теме, обсуждение ее, формулирование выводов и заключения).

На занятиях семинарского типа докладчики готовят реферат, презентацию и доклад по центральной теме семинара.

После доклада все участники семинара задают вопросы, на которые отвечают докладчик и другие члены группы. Вопросы и ответы составляют центральную часть семинара. Оценивается качество реферата, качество доклада, качество презентации, активность в участии в работе семинара, качество ответов на вопросы.

Ход занятий:

Семинар (90 минут) состоит из 3 логических частей:

1. Доклад по центральной теме семинара, около 45 минут – группа Докладчиков.
2. Вопросы аудитории по докладу – около 15–20 минут. Вопросы задают студенты и преподаватель.
3. Дискуссия. После ответов на вопросы происходят обсуждения по теме семинара 25–30 минут, развертывается дискуссия по проблемам, поднятым в работе. Производится подведение итогов.

Описание заданий на семинар для всех групп участников

Часть 1. Основная часть семинара

Группе докладчиков к занятию необходимо предоставить реферат, презентацию и подготовить общий групповой доклад. Важно, чтобы материалы разных авторов не повторялась ни в реферате, ни в ходе доклада. Контроль данного вопроса производит руководитель группы.

Реферат по центральной теме семинара заранее (за 2–3 дня до занятия) передается для ознакомления преподавателю.

Основная часть реферата состоит из разделов, написанных каждым участником группы (1 раздел – 1 автор). Каждый раздел представляет собой, по сути, микроисследование.

Презентация и доклад по теме семинара. Доклад носит характер полного аргументированного изложения центральной темы семинарского занятия. Излагают сущность исследования, защищаемой точки зрения, собственные позиции. Аргументируют, обосновывают, иллюстрируют позицию.

Часть 2 и Часть 3. Вопросы и дискуссия

В ходе семинара слушатели готовят вопросы докладчикам, которые они задают группе выступающих после доклада. Любой вопрос может быть переадресован слушателям семинара. Как известно, способность поставить вопрос предполагает подготовленность по соответствующей теме. И чем основательнее подготовка, тем более глубокие и квалифицированные вопросы задаются. Поэтому все студенты к занятию готовят подборку интересной современной литературы, новых книг, научных статей или новостей по теме семинара, а также интересующие их вопросы, относящиеся к теме семинара.

Активность слушателей поощряется и оценивается дополнительно. Для получения дополнительной оценки за семинар необходимо проявить активность в его работе, подготовить и участвовать в дискуссии по подготовленным вопросам. Оценивается умение задавать хорошо продуманные, четко сформулированные дополнительные вопросы.

На основе вопросов и ответов развертывается дискуссия.

В конце занятия производится подведение итогов, оцениваются выступления докладчиков и всех остальных участников семинара, оценивается продуктивность всей дискуссии, правомерность выдвинутых гипотез и предложений, сделанных выводов, высказывается мнение о вкладе того или иного участника дискуссии в нахождение общего решения и т.д.

Оценка работы на семинаре

Докладчики

Оценивается:

a. качество реферата в целом (логичность, последовательность, актуальность материала) – 0 / 3 / 4 / 5 – групповая оценка;
b. качество доклада в целом (логичность, последовательность, наличие выводов) – 0 / 3 / 4 / 5 – групповая оценка;
c. качество презентации в целом (логичность, последовательность, наличие выводов) – 0 / 3 / 4 / 5 – групповая оценка;
d. качество представленного материала – 0 / 3 / 4 / 5 – индивидуальная оценка;
e. качество доклада (доклад был произведен самостоятельно, представлен логично) – 0 / 3 / 4 / 5 – индивидуальная оценка;
f. качество презентации (помогает ли презентация в восприятии материала, содержит ли графический материал, наглядные изображения)– 0 / 3 / 4 / 5 – индивидуальная оценка;
g. активность в участии в работе семинара 0 / 3 / 4 / 5 – индивидуальная оценка;

h. качество ответов на вопросы 0 / 3 / 4 / 5 – групповая и индивидуальная оценка.

Остальные участники

Активность поощряется и оценивается дополнительно. Для получения оценки за семинар необходимо проявить активность в его работе, подготовить и участвовать в дискуссии по подготовленным вопросам. Оценивается умение задавать хорошо продуманные, четко сформулированные дополнительные вопросы.

Оценивается:

a. Активность в работе на семинаре 0 / 3 / 4 / 5 – индивидуальная оценка;
b. Качество вопросов 0 / 3 / 4 / 5 – индивидуальная оценка.

ПЕРЕЧЕНЬ КОНТРОЛЬНЫХ ВОПРОСОВ

1. Европейская Конвенция по борьбе с киберпреступностью. Виды и составы компьютерных преступлений.
2. Директивы и регламенты ЕС по противодействию киберпреступности.
3. Защита государственной тайны в США.
4. Защита государственной тайны в европейских странах (Великобритания, Германия, Франция).
5. Защита государственной тайны в странах Азии и Дальнего Востока.
6. Национальное законодательство США по противодействию компьютерным преступлениям. Правовые основы информационной безопасности. Законодательство в области компьютерных преступлений. Расследование компьютерных преступлений. Состав и основные направления деятельности органов защиты информации.
7. Национальные законодательства стран ЕС по противодействию компьютерным преступлениям. Правовые основы информационной безопасности. Законодательство в области компьютерных преступлений. Расследование компьютерных преступлений. Состав и основные направления деятельности органов защиты информации.
8. Национальные законодательства стран Азии и Дальнего Востока (КНР, Япония, Индия, Сингапур) по противодействию компьютерным преступлениям. Правовые основы информационной безопасности. Законодательство в области компьютерных преступлений. Расследование компьютерных преступлений. Состав и основные направления деятельности органов защиты информации.

ВОПРОСЫ ДЛЯ САМОСТОЯТЕЛЬНОГО ОЗНАКОМЛЕНИЯ

Представлены темы дополнительных рефератов и статей. Перечень тем дополняется преподавателем.

1. Законодательства о компьютерных преступлениях:
    a. национальное законодательство (в том числе прецедентное право): материально-уголовное и процессуальное право.
    b. международные и двухсторонние соглашения. Юрисдикция. Каналы судебного и оперативного сотрудничества.

2. Электронные доказательства: основные понятия, требования и компьютерная криминалистическая экспертиза, технические и уголовно-процессуальные процедуры. Методы поиска, изъятия и хранения электронных доказательств;

3. Каналы судебного и оперативного сотрудничества;

4. Выявление подозреваемых лиц.

5. История Эдварда Сноудена.

6. Законодательства о компьютерных преступлениях: международные и двухсторонние соглашения. Юрисдикция. Каналы судебного и оперативного сотрудничества.

7. Международная защита интеллектуальной собственности.

РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА

Основная литература:

1. Алпеев А. С. Терминология безопасности: кибербезопасность, информационная безопасность //Вопросы кибербезопасности. – 2014. – №. 5 (8).

2. Анурьева М. С. Подходы к формированию содержания дисциплин по правовой защите информации за рубежом //Гаудеамус. – 2014. – №. 2 (24).

3. Бородакий Ю. В., Добродеев А. Ю., Бутусов И. В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 2) //Вопросы кибербезопасности. – 2014. – №. 1 (2).

4. Быков В. М., Черкасов В. Н. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы. – 2015.

5. Дунъян Ч. Современное состояние цифровой экономики в Китае и перспективы сотрудничества между Китаем и Россией в области цифровой экономики //Власть. – 2017. – №. 9.

6. Международная информационная безопасность: монография / Е.С.Зиновьева; Моск. гос. ин-т междунар. Отношений (ун-т) МИД России, каф. мировых политических процессов. — М. : МГИМО-Университет, 2013. — 194 с. — Серия «Научная школа МГИМО». ISBN 978-5-9228-1018-0)

7. Коноваленко с. А. Проблемы и перспективы внедрения форензики как метода выявления фактов мошенничества и злоупотреблений должностными лицами //теоретические и практические проблемы развития уголовно-исполнительной системы в российской федерации и за рубежом. – 2018. – С. 1409-1415.

8. Крылова И. А. Новые виды войн и безопасность России //Знание. Понимание. Умение. – 2016. – №. 3.

9. Леонтьев Б. К. Хакеры, взломщики и другие информационные убийцы [Москва: Майор (Осипенко), 2001 – 190 с.].

10. Марков А. С., Цирлов В. Л. Руководящие указания по кибербезопасности в контексте ISO 27032 //Вопросы кибербезопасности. – 2014. – №. 1 (2).

11. Мухамедзянов Г. И. Форензика. Свободное программное обеспечение в расследовании инцидентов информационной безопасности //Научно-техническая конференция студентов, аспирантов и молодых специалистов НИУ ВШЭ им. ЕВ Арменского. – 2015. – С. 148-148.

12. Рябчук В. Государственная измена и шпионаж. Уголовно-правовое и криминологическое исследование. – Litres, 2017.

Дополнительная литература

13. Аверченков В. И. и др. Системы защиты информации в ведущих зарубежных странах. – 2012.

14. Громов Е. В. Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритании, ФРГ, Нидерландах, Польше) //Вестник Томского государственного педагогического университета. – 2006. – №. 11.

15. Ибрагимова Г. Стратегия КНР в области управления интернетом и обеспечения информационной безопасности //Индекс безопасности. – 2013. – Т. 19. – №. 1. – С. 170.

16. Карамнов А. Ю., Дворецкий М. Ю. Уголовная ответственность за преступления в сфере компьютерной информации в России и зарубежных государствах //Вестник Воронежского института МВД России. – 2011. – №.

17. Медведев И. В. Компьютерная криминалистика «форензика» и киберпреступность в России //Пролог: журнал о праве. – 2013. – №. 3.

18. Чванова М. С., Анурьева М. С. Подготовка кадров в области информационной безопасности в США //Вестник Тамбовского университета. Серия: Гуманитарные науки. – 2012. – Т. 112. – №. 8.

19. Чванова М. С., Анурьева М. С. Подготовка специалистов в области информационной безопасности во Франции //Вестник Тамбовского университета. Серия: Гуманитарные науки. – 2012. – Т. 111. – №. 7.

Ссылки на электронные ресурсы, используемые в практических работах:

20. Государственные стратегии кибербезопасности URL: https://www.securitylab.ru/analytics/429498.php (дата обращения: 24.11.2019).
21. Законодательство Франции в сфере защиты персональных данных и информационной безопасности URL: http://uipdp.com/solutions/services/consulting/legislation/eu/france.html (дата обращения: 24.11.2019).
22. Закон КНР о защите государственной тайны URL: http://www.asia-business.ru/law/law3/secret/#3 (дата обращения: 24.11.2019).
23. Япония: закон о гостайне URL: http://ru.journal-neo.org/2014/12/16/yaponiya-zakon-o-gostajne/ (дата обращения: 24.11.2019).
24. Закон об охране государственной тайны вступил в силу в Японии URL: http://ria.ru/world/20141210/1037433129.html (дата обращения: 24.11.2019).
25. Методика расследования утраты документов содержащих военную тайну URL: http://refleader.ru/merujgujgyfs.html (дата обращения: 24.11.2019).
26. Наказания за выдачу секретной информации в разных странах URL: http://ria.ru/spravka/20080117/97167181.html (дата обращения: 24.11.2019).

27. История одной защиты URL: http://samlib.ru/i/iwanow_n/istorijaodnojzashity.shtml (дата обращения: 24.11.2019).
28. Cybercrime laws from around the world URL: https://www.cybercrimelaw.net/Cybercrimelaws.html (дата обращения: 24.11.2019).
29. Federal Computer Crime Laws URL: https://www.sans.org/reading-room/whitepapers/legal/federal-computer-crime-laws-1446 (дата обращения: 24.11.2019).
30. Мировые стратегии кибербезопасности URL: http://d-russia.ru/mirovye-strategii-kiberbezopasnosti.html (дата обращения: 24.11.2019).
31. Глобальный индекс кибербезопасности и профили по киберблагополучию // Международный союз электросвязи URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-R.pdf (дата обращения: 24.11.2019).
32. Good Practice Guide on National Cyber Security Strategies URL: https://www.enisa.europa.eu/publications/ncss-good-practice-guide (дата обращения: 24.11.2019).
33. Стратегия национальной кибербезопасности Соединенных Iтатов Америки URL: http://d-russia.ru/wp-content/uploads/2019/01/National-Cyber-Strategy_USA_2018.pdf (дата обращения: 24.11.2019).
34. Подходы Японии к кибербезопасности. Как реагировать на неопределенность? URL: https://digital.report/podhodyi-yaponii-k-kiberbezopasnosti-2/ , https://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf (дата обращения: 24.11.2019).
35. Cyber Security Strategy for Germany URL: http://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1 (дата обращения: 24.11.2019).
36. The National Cyber Security Strategy (NCSS) of Netherlands URL: http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011 (дата обращения: 24.11.2019).
37. Cyber Security Strategy of the United Kingdom URL: http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf (дата обращения: 24.11.2019).
38. Finland´s Cyber security Strategy URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf9 (дата обращения: 24.11.2019).
39. Défense et sécurité des systèmes d'informationStratégie de la France URL: http://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011 (дата обращения: 24.11.2019).
40. CYBER SECURITY STRATEGY OF THE CZECH REPUBLIC FOR THE 2011 – 2015 PERIOD URL: http://www.enisa.europa.eu/media/news-

items/CZ_Cyber_Security_Strategy_20112015.PDF (дата обращения: 24.11.2019).
41. Estonian National Cyber Security Strategy: URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy (дата обращения: 24.11.2019).

Приложение 1. Советы Cisco по кибербезопасности

1. Поймите, что вы привлекательная цель для хакеров. Никогда не говорите «это не случится со мной».

2. Управляйте паролями. Не используйте один и тот же пароль для нескольких сайтов. Используйте разные регистры и дополнительные символы. Не делитесь своим паролем с другими, не записывайте его и, конечно же, не прикрепляйте стикер с паролем к вашему монитору.

3. Никогда не оставляйте свои устройства без присмотра. Если вам нужно оставить свой компьютер, телефон или планшет на какое-то время. неважно, насколько короткое – заблокируйте его, чтобы никто не мог использовать его, пока вас нет.

4. Всегда будьте осторожны при открытии вложений или ссылки в электронной почте. Проверяйте адрес отправителя сообщения и URL-адрес веб-сайта, на который ведет ссылка: злоумышленники часто используют орфографические ошибки, чтобы направить вас на похожий по адресу, но вредоносный домен.

5. Доступ к конфиденциальной информации (онлайн банкинг или покупки), должен выполняться только на устройстве, которое принадлежит вам, в сети, которой вы доверяете. Смартфон друга или коллеги по работе, общественный компьютер или бесплатный Wi-Fi в кафе или метро – учитывайте, что ваши данные могут быть скопированы или украдены.

6. Регулярно создавайте резервные копии данных и проверяйте, что загружена актуальная версия антивирусного программного обеспечение. Помните, что все операционные системы подвергаются атакам.

7. Не подключайте к компьютеру сомнительные устройства. Вредоносное ПО может распространяться через зараженные флэш-накопители, внешние жесткие диски и даже смартфоны.

8. Думайте о том, чем вы делитесь в социальных сетях. Преступники могут подружиться с вами и легко получить доступ к шокирующему количеству информации – где вы учитесь, где работаете, когда находитесь в отпуске, – что может помочь им получить доступ к более ценным данным.

9. Будьте готовы к тому, что кто-то захочет получить от вас информацию с помощью методов социальной инженерии, например, с помощью манипуляций. Если кто-то звонит или пишет вам по электронной почте с просьбой предоставить конфиденциальную информацию или перевести деньги на неизвестный вам счет, вы можете сказать «нет». Вы всегда можете позвонить в компанию или человеку напрямую, чтобы проверить учетные данные, прежде чем выдавать какую-либо информацию.

10. Обязательно контролируйте свои учетные записи на предмет любых подозрительных действий. Если вы заметили какие-то несанкционированные изменения, это может быть признаком того, что ваша учетная запись была скомпрометирована.

Воробьева Алиса Андреевна

Коржук Виктория Михайловна

Системы защиты информации в ведущих зарубежных странах

Часть 2

Учебно-методическое пособие

В авторской редакции
Редакционно-издательский отдел Университета ИТМО
Зав. РИО Н.Ф. Гусарова
Подписано к печати
Заказ №
Тираж
Отпечатано на ризографе

Редакционно-издательский отдел
Университета ИТМО
197101, Санкт-Петербург, Кронверский пр., 49