Литература

Основная.

1. **Урбанович П.П. Защита информации методами криптографии, стеганографии и обфускации. – Минск: БГТУ, 2016**
2. Урбанович П. П., Шиман Д. В., Шутько Н. П. Лабораторный практикум по дисциплинам "Защита информации и надежность информационных систем" и "Криптографические методы защиты информации". В 2 ч. Ч. 1. Кодирование информации : учебно-методическое пособие для студентов учреждений высшего образования. – Минск: БГТУ, 2019. – 116 с.
3. Урбанович П. П., Шутько Н. П. Лабораторный практикум по дисциплинам «Защита информации и надежность информационных систем» и «Криптографические методы защиты информации». В 2 ч. Ч. 2. Криптографические и стеганографические методы защиты информации: учеб.-метод. пособие для студ. иузов.– Минск: БГТУ, 2020. – 226 с.
4. Урбанович П.П., Шиман Д.В. Защита информации и надежность информационных ситем / Учебно-методическое пособие.- Мн.:БГТУ, 2014.

Дополнительная.

1. М.Ховард, Д.Лебланк. *Защищенный код*. – М.: Издательский дом «Русская редакция», 2005.
2. Б. Шнайер. Прикладная криптография. – М.: Триумф, 2003.
3. Харин Ю. С., Берник В. И., Матвеев Г.В. *Математические основы криптологии*. - Мн. :БГУ, 1999.
4. Черкесов Г.Н. *Надежность аппаратно-программных комплексов*. – Питер,2005.
5. Д.Фористайл. *Защита от хакеров*. – М.:ДМК Пресс, 2003.
6. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. – ИД «Форум»-Инфра-М, 2008

7. К. Митник. Искусство обмана (социальный инженерия)
8. К. Митник. Искусство вторжения
9. К. Митник. Призрак в сети.
10. К. Митник. Искусство быть невидимым.
11. Дж. Эриксон. Хакинг. Искусство эксплойта

Основные понятия и определения 1

Информация – сведения (данные) о внутреннем и окружающем нас мире, событиях, процессах, явлениях и т.д., воспринимаемые и передаваемые людьми или техническими устройствами.

Информационная (информационно-вычислительная) система – организационно упорядоченная совокупность документов, технических средств и информационных технологий, реализующая информационные (информационно-вычислительные) процессы.

Информационные процессы – процессы сбора, накопления, хранения, обработки (переработки), передачи и использования информации.

Информационные ресурсы – отдельные документы или массивы документов в информационных системах.

Информационные технологии (**ИТ**, также — информационно-коммуникационные технологии) — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов ;

Доступ – специальный тип взаимодействия между объектом и субъектом, в результате которого создается поток информации от одного к другому.

Несанкционированный доступ – доступ к информации, устройствам ее хранения и обработки, а также к каналам передачи, реализуемый без ведома (санкции) владельца и нарушающий тем самым установленные правила доступа.

Объект – пассивный компонент системы, хранящий, перерабатывающий, передающий или принимающий информацию; примеры объектов: страницы, файлы, папки, директории, компьютерные программы, устройства (мониторы, диски, принтеры и т.д.)

Субъект – активный компонент системы , который может инициировать поток информации; примеры субъектов: пользователь, процесс либо устройство.

Безопасность ИВС – свойство системы, выражающееся в способности системы противодействовать попыткам несанкционированного доступа или нанесения ущерба владельцам и пользователям системы при различных умышленных и неумышленных воздействиях не нее.

Защита информации – организационные, правовые, программно-технические и иные меры по предотвращению угроз информационной безопасности и устранению их последствий.

Информационная безопасность систем – свойство информационной системы или реализуемого в ней процесса, характеризующее способность обеспечить необходимый уровень своей защиты.

Информационная безопасность (*information security*) — все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности информации или средств её обработки (**CIA**):

конфиденциальность (***C****onfidentiality*) — состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на нее право;

целостность (***I****ntegrity*) — избежание несанкционированной модификации информации;

доступность (***A****vailability*) — избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

понятие **«информационная безопасность»** рассматривается в следующих значениях:

- **состояние (качество)** определённого объекта (в качестве объекта может выступать информация, данные, ресурсы автоматизированной системы, автоматизированная система, информационная система предприятия, общества, государства и т. п.);
- **деятельность**, направленная на обеспечение защищённого состояния объекта (в этом значении чаще используется термин **«защита информации»**

Надежность системы – характеристика способности программного, аппаратного, аппаратно-программного средства выполнить при определенных условиях требуемые функции в течение определенного периода времени.

Достоверность работы системы (устройства) – свойство, характеризующее истинность конечного (выходного) результата работы (выполнения программы), определяемое способностью средств контроля фиксировать правильность или ошибочность работы.

Ошибка устройства – неправильное значение сигнала (бита – в цифровом устройстве) на внешних выходах устройства или отдельного его узла, вызванное технической неисправностью или воздействующими на него помехами (преднамеренными либо непреднамеренными).

Ошибка программы – проявляется в не соответствующем реальному (требуемому) промежуточному или конечному значению (результату) вследствие неправильно запрограммированного алгоритма или неправильно составленной программы.

Составляющие ИБ:

1. Законодательная, нормативно-правовая и научная база.
2. Организационно-технические и режимные меры и методы (Политика информационной безопасности).

3. Программно-технические и программные способы и средства обеспечения ИБ

Нормативные документы в области информационной безопасности

Акты национального законодательства:

- Международные договоры РБ;
- Конституция РБ;
- Законы РБ;
- Указы Президента РБ;
- Постановления правительства РБ;
- Нормативные правовые акты министерств и ведомств;
- Нормативные правовые акты субъектов, органов местного самоуправления и т. д

Международные стандарты:

BS 7799-1:2005 — Британский стандарт BS 7799 Part 1 — Code of Practice for Information Security Management (Практические правила управления информационной безопасностью) описывает 127 механизмов контроля, необходимых для построения *системы управления информационной безопасностью* организации, определённых на основе лучших примеров мирового опыта в данной области. Этот документ служит практическим руководством по созданию СУИБ

BS 7799-2:2005 — Британский стандарт BS 7799 Part 2 — Information Security management — specification for information security management systems (Спецификация системы управления информационной безопасностью) определяет спецификацию СУИБ. Вторая часть стандарта используется в качестве критериев при проведении официальной процедуры сертификации СУИБ организации.

ISO/IEC 17799:2005 — «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности». Международный стандарт, базирующийся на BS 7799-1:2005.

ISO/IEC 27001:2005 — «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования». Международный стандарт, базирующийся на BS 7799-2:2005.

ISO/IEC 27001 (ISO 27001) - собраны описания лучших мировых практик в области управления информационной безопасностью. ISO 27001 устанавливает требования к системе менеджмента ИБ для демонстрации способности организации защищать свои информационные ресурсы. Этот стандарт подготовлен в качестве модели для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы менеджмента информационной безопасности.

ISO/IEC 27002 — Сейчас: ISO/IEC 17799:2005. «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности». Дата выхода — 2007 год.

ISO/IEC 27005 — Сейчас: BS 7799-3:2006 — Руководство по менеджменту рисков ИБ.

Нормативные правовые акты в области обеспечения информационной безопасности

- Постановление Совета Министров Республики Беларусь от 11 февраля 2006 г. №192 "Об утверждении Положения о сопровождении интернет-сайтов республиканских органов государственного управления, иных государственных организаций, подчиненных Правительству Республики Беларусь",
- Закон Республики Беларусь от 10 ноября 2008 г. №455-З «Об информации, информатизации и защите информации»,

Закон Республики Беларусь № 455-З от 10 ноября 2008 г.
Об информации, информатизации и защите информации

Указ № 515 Президента Республики Беларусь от 30 сентября 2010 г.
О некоторых мерах по развитию сети передачи данных в Республике Беларусь

Указ № 60 Президента Республики Беларусь от 1 февраля 2010 г.
О мерах по совершенствованию использования национального сегмента сети Интернет

Постановление № 1084 Совета Министров Республики Беларусь от 11 августа 2011 г.
О внесении изменений и дополнений в постановление Совета Министров Республики Беларусь от 29 апреля 2010 г. № 644

Постановление № 675 Совета Министров Республики Беларусь от 26 мая 2009 г. О некоторых вопросах защиты информации

Постановление № 673 Совета Министров Республики Беларусь от 26 мая 2009 г.
О некоторых мерах по реализации Закона Республики Беларусь "Об информации, информатизации и защите информации" и о признании утратившими силу некоторых постановлений Совета Министров Республики Беларусь

Постановление № 644 Совета Министров Республики Беларусь от 29 апреля 2010 г.
О некоторых вопросах совершенствования использования национального сегмента глобальной сети Интернет

Постановление № 670 Совета Министров Республики Беларусь от 6 ноября 1992 г. Об утверждении положения о коммерческой тайне

Постановление № 4/11 Оперативно-аналитического центра при Президенте Республики Беларусь и Министерства связи и информатизации Республики Беларусь от 29 июня 2010 г.
Об утверждении положения о порядке ограничения доступа пользователей интернет-услуг к информации, запрещенной к распространению в соответствии с законодательными актами

Приказ № 60 Оперативно-аналитического центра при Президенте Республики Беларусь от 2 августа 2010 г.
Об утверждении положения о порядке определения поставщиков интернет-услуг, уполномоченных оказывать интернет-услуги государственным органам и организациям, использующим в своей деятельности сведения, составляющие государственные секреты

УКАЗ ПРЕЗИДЕНТА РЕСПУБЛИКИ БЕЛАРУСЬ
9 ноября 2010 г. № 575 : Об утверждении Концепции национальной безопасности Республики Беларусь

Тенденция: Информационная сфера превращается в системообразующий фактор жизни людей, обществ и государств

Информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере

Основные национальные интересы в области ИТ:

-реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации;
- формирование и поступательное развитие информационного общества; равноправное участие Республики Беларусь в мировых информационных отношениях;
- преобразование информационной индустрии в экспортно-ориентированный сектор экономики;
- эффективное информационное обеспечение государственной политики;
- обеспечение надежности и устойчивости функционирования критически важных объектов информатизации.

Внутренние источники угроз национальной безопасности:

- распространение недостоверной или умышленно искаженной информации, способной причинить ущерб национальным интересам Республики Беларусь;
- зависимость Республики Беларусь от импорта информационных технологий, средств информатизации и защиты информации, неконтролируемое их использование в системах, отказ или разрушение которых может причинить ущерб национальной безопасности;
- несоответствие качества национального контента мировому уровню;
- недостаточное развитие государственной системы регулирования процесса внедрения и использования информационных технологий;
- рост преступности с использованием информационно-коммуникационных технологий;
- недостаточная эффективность информационного обеспечения государственной политики;
- несовершенство системы обеспечения безопасности критически важных объектов информатизации.

Внешние источники угроз национальной безопасности:

- открытость и уязвимость информационного пространства Республики Беларусь от внешнего воздействия;
- доминирование ведущих зарубежных государств в мировом информационном пространстве, монополизация ключевых сегментов информационных рынков зарубежными информационными структурами;
- информационная деятельность зарубежных государств, международных и иных организаций, отдельных лиц, наносящая ущерб национальным интересам Республики Беларусь, целенаправленное формирование информационных поводов для ее дискредитации;
- нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве;
- развитие технологий манипулирования информацией;
- препятствование распространению национального контента Республики Беларусь за рубежом;
- широкое распространение в мировом информационном пространстве образцов массовой культуры, противоречащих общечеловеческим и национальным духовно-нравственным ценностям;
- попытки несанкционированного доступа извне к информационным ресурсам Республики Беларусь, приводящие к причинению ущерба ее национальным интересам.

ПОСТАНОВЛЕНИЕ СОВЕТА МИНИСТРОВ РЕСПУБЛИКИ БЕЛАРУСЬ

9 августа 2010 г. № 1174: О Стратегии развития информационного общества в Республике Беларусь на период до 2015 года и плане первоочередных мер по реализации Стратегии развития информационного общества в Республике Беларусь на 2010 год

информатизация – организационный, социально-экономический и научно-технический процесс, обеспечивающий условия для формирования и использования информационных ресурсов и реализации информационных отношений;

информационная система – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств;

информационная технология – совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и защиты информации;

Приоритетными направлениями деятельности в области обеспечения информационной безопасности являются:

- развитие правового обеспечения информационной безопасности и совершенствование правоохранительной деятельности в этой сфере;
- разработка и внедрение эффективных программных и программно-аппаратных средств защиты информационных ресурсов, информационных и телекоммуникационных систем;
- создание централизованно управляемой ИКИ, необходимой для обеспечения деятельности государственных органов, включая соответствующий уровень защиты информации;
- увеличение набора в высшие учебные заведения на специальности в области защиты информации, совершенствование системы повышения квалификации и создание системы переподготовки кадров в этой области;
- формирование системы мониторинга информационной безопасности Республики Беларусь в наиболее важных сферах жизнедеятельности общества и государства.

Организационно-технические и режимные меры и методы

Для построения Политики ИБ рассматривают следующие направления защиты информационной системы (ИС)

- Защита объектов ИС;
- Защита процессов, процедур и программ обработки информации;
- Защита каналов связи;
- Подавление побочных электромагнитных излучений;
- Управление системой защиты.

Организационная защита обеспечивает:

- организацию охраны, режима, работу с кадрами, с документами;
- использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз

Правовая защита информации

- **Правовой элемент** системы организации защиты информации на предприятии основывается на нормах информационного права и предполагает юридическое закрепление взаимоотношений фирмы и государства по поводу правомерности использования системы защиты информации, фирмы и персонала по поводу обязанности персонала соблюдать установленные меры защитного характера, ответственности персонала за нарушение порядка защиты информации.
- **Правовая защита включает**:

— наличие в организационных документах фирмы, правилах внутреннего трудового распорядка, трудовых договорах, в должностных инструкциях положений и обязательств по защите конфиденциальной информации;

— формулирование и доведение до сведения всех сотрудников положения о правовой ответственности за разглашение конфиденциальной информации, несанкционированное уничтожение или фальсификацию документов;

— разъяснение лицам, принимаемым на работу, положения о добровольности принимаемых ими на себя ограничений, связанных с выполнением обязанностей по защите информации.

Основные подсистемы защиты информации в правовом плане:

— установление на объекте режима конфиденциальности;

— разграничение доступа к информации;

— правовое обеспечение процесса защиты информации;

— четкое выделение конфиденциальной информации как основного объекта защиты.

Собственные нормативно- правовые документы предприятия, ориентированные на обеспечение информационной безопасности:

Политика Информационной безопасности;

Положение о коммерческой тайне;

Положение о защите персональных данных;

Перечень сведений, составляющих конфиденциальную информацию;

Инструкция о порядке допуска сотрудников к сведениям, составляющим конфиденциальную информацию;

Положение о специальном делопроизводстве и документообороте;

Обязательство сотрудника о сохранении конфиденциальной информации;

Памятка сотруднику о сохранении коммерческой тайны.

Компьютерное преступление

- **КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ** (computer crime) **-** любое противоправное действие, при котором компьютер выступает либо как объект, против которого совершается преступление, либо как инструмент, используемый для совершения преступных действий.
- **Термин «компьютерное пиратство»** обозначает **нарушение авторских прав** на программное обеспечение (ПО). Такое нарушение возникает при несанкционированном правообладателем копировании, использовании и распространении программного обеспечения.
- **5 видов пиратства**
- Незаконное копирование конечными пользователями
- Незаконная установка программ на жесткие диски компьютеров
- Изготовление подделок
- Нарушение ограничений лицензии
- Интернет-пиратство

КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ ПО КОДИФИКАТОРУ МЕЖДУНАРОДНОЙ УГОЛОВНОЙ ПОЛИЦИИ ГЕНЕРАЛЬНОГО СЕКРЕТАРИАТА ИНТЕРПОЛА

- В 1991 году данный **кодификатор** был интегрирован в автоматизированную систему поиска и в настоящее время доступен подразделениям Национальных центральных бюро Международной уголовной полиции "Интерпол" более чем 120 стран мира.

  Все коды характеризующие компьютерные преступления имеют идентификатор, начинающийся с буквы **Q**.

- Для характеристики преступления могут использоваться до пяти кодов, расположенных в порядке убывания значимости совершенного.

- **QA - НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП И ПЕРЕХВАТ**

  QAH - компьютерный абордаж (**hacking** - "хакинг"): доступ в компьютер или сеть без права на то. Этот вид компьютерных преступлений обычно используется преступниками для проникновения в чужие информационные сети.

  QAI – перехват (**interception**): перехват при помощи технических средств, без права на то. Перехват информации осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. К данному виду компьютерных преступлении также относится **электромагнитный перехват** (electromagnetic pickup).

  QA1 - кража времени заключается в неоплате услуг доступа в систему или сеть ЭВМ

  QAZ - прочие виды несанкционированного доступа и перехвата

  QD - ИЗМЕНЕНИЕ КОМПЬЮТЕРНЫХ ДАННЫХ

  QDL - логическая бомба

  QDT - троянский конь

  QDV - компьютерный вирус

  QDW - компьютерный червь

  QDZ - прочие виды изменения данных

QF - КОМПЬЮТЕРНОЕ МОШЕННИЧЕСТВО (COMPUTER FRAUD)

QFC - мошенничество с банкоматами

QFF - компьютерная подделка

QFG - мошенничество с игровыми автоматами

QFM - манипуляции с программами ввода вывода

QFP - мошенничества с платежными средствами

QFT - телефонное мошенничество

QFZ - прочие компьютерные мошенничества

QR - НЕЗАКОННОЕ КОПИРОВАНИЕ ("ПИРАТСТВО")

QRG - компьютерные игры

QRS - прочее программное обеспечение

QRT - топография полупроводниковых изделий

QRZ - прочее незаконное копирование

- **QS - КОМПЬЮТЕРНЫЙ САБОТАЖ**
  QSH - с аппаратным обеспечением
  QSS - с программным обеспечением
  QSZ - прочие виды саботажа
- **QZ - ПРОЧИЕ КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ**
  QZB - с использованием компьютерных досок объявлении
  QZE - хищение информации, составляющей коммерческую тайну
  QZS - передача информации конфиденциального характера
  QZZ - прочие компьютерные преступления

- Согласно **ст.34 Конституции РБ** «пользование информацией может быть ограничено законодательством в целях защиты чести, достоинства, личной и семейной жизни граждан». Согласно **ст.21 Конституции РБ «**каждый имеет право на защиту от незаконного вмешательства в его личную жизнь, в том числе от посягательства на тайну его корреспонденции и иных сообщений. Защите подлежит любая документальная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу или пользователю.
- Собственник документов информационных систем устанавливает порядок предоставления пользователю всей информации с указанием места, времени, ответственности должностных лиц, а также необходимых процедур и обеспечивают условия доступа пользователей информации.

- # Кодекс *Республики Беларусь* об административных правонарушениях

ГЛАВА 23

ПРЕСТУПЛЕНИЯ ПРОТИВ КОНСТИТУЦИОННЫХ ПРАВ И СВОБОД ЧЕЛОВЕКА И ГРАЖДАНИНА

Статья 201. Нарушение авторских, смежных, изобретательских и патентных прав

- 1. Присвоение авторства либо принуждение к соавторству, а равно разглашение без согласия автора или заявителя сущности изобретения, полезной модели, промышленного образца или иного объекта права промышленной собственности до официальной публикации сведений о них – ***наказываются общественными работами, или штрафом, или исправительными работами на срок до двух лет***.
- 2. Незаконное распространение или иное незаконное использование объектов авторского права, смежных прав или объектов права промышленной собственности, совершенные в течение года после наложения административного взыскания за такое же нарушение или сопряженные с получением дохода в крупном размере, – ***наказываются общественными работами, или штрафом, или ограничением свободы на срок до трех лет, или лишением свободы на срок до двух лет.***
- 3. Действия, предусмотренные частями первой или второй настоящей статьи, совершенные повторно, либо группой лиц по предварительному сговору, либо должностным лицом с использованием своих служебных полномочий, либо повлекшие причинение ущерба в крупном размере, – ***наказываются штрафом, или арестом на срок до шести месяцев, или ограничением свободы на срок до пяти лет, или лишением свободы на тот же срок.***

- Примечание. Крупным размером дохода (ущерба) в настоящей статье признается размер дохода (ущерба) на сумму, в пятьсот и более раз превышающую размер базовой величины, установленный на день совершения преступления.

Программно-технические способы и средства обеспечения информационной безопасности

- **Средства защиты от несанкционированного доступа** (НСД):
  Средства авторизации;
  Аудит;
- **Системы мониторинга сетей**:
  Системы мониторинга сетей;
  Анализаторы протоколов;
- **Антивирусные средства**

Межсетевые экраны

- **Криптографические средства**
- **Системы бесперебойного питания**
- **Системы аутентификации**:
- Пароль;
- Ключ доступа (физический или электронный);
- Биометрия.