Методы и средства защиты информации

Основы информационной безопасности

Методы и средства

Защита как инвестиция в будущее

Средний размер ущерба в результате одного инцидента ИБ для компаний **среднего бизнеса** РФ составляет **1,6 млн**. рублей, а для **крупного бизнеса** он в десять раз выше – **16,1 млн. рублей**.

Современной антивирусной программы уже недостаточно – необходимо комплексное решение, отвечающее за безопасность на нескольких технологических и функциональных уровнях корпоративной IT-инфраструктуры.

Истинная защита рабочих мест сочетает в себе различные интеллектуальные методы и технологии для защиты от любых киберугроз на любой платформе. Обезопасив всю корпоративную IT-сеть, вы сможете обеспечить непрерывность бизнеса. [Kaspersky, 2020]

Методы и средства защиты информации

- **Реализация вопросов ИБ тесна связана не только с технической и программной реализацией, но и нормативно-правовой.**
- Благодаря интернету во всем мире стираются границы и в виртуальном пространстве люди, «роботы», программы действуют вне границ следовательно необходимо учитывать не только национальную правовую базу, но и также основных мировых государств (Россия, **Беларус**США, Китай, Европа).
- Поэтому **в лекционном курсе будет даваться информация по Миру в целом, России, Беларуси, США, Китаю, Европейским странам.**

Рекомендуемая литература

Защита информации : учебное пособие / А.П. Жук, Е. П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1210523

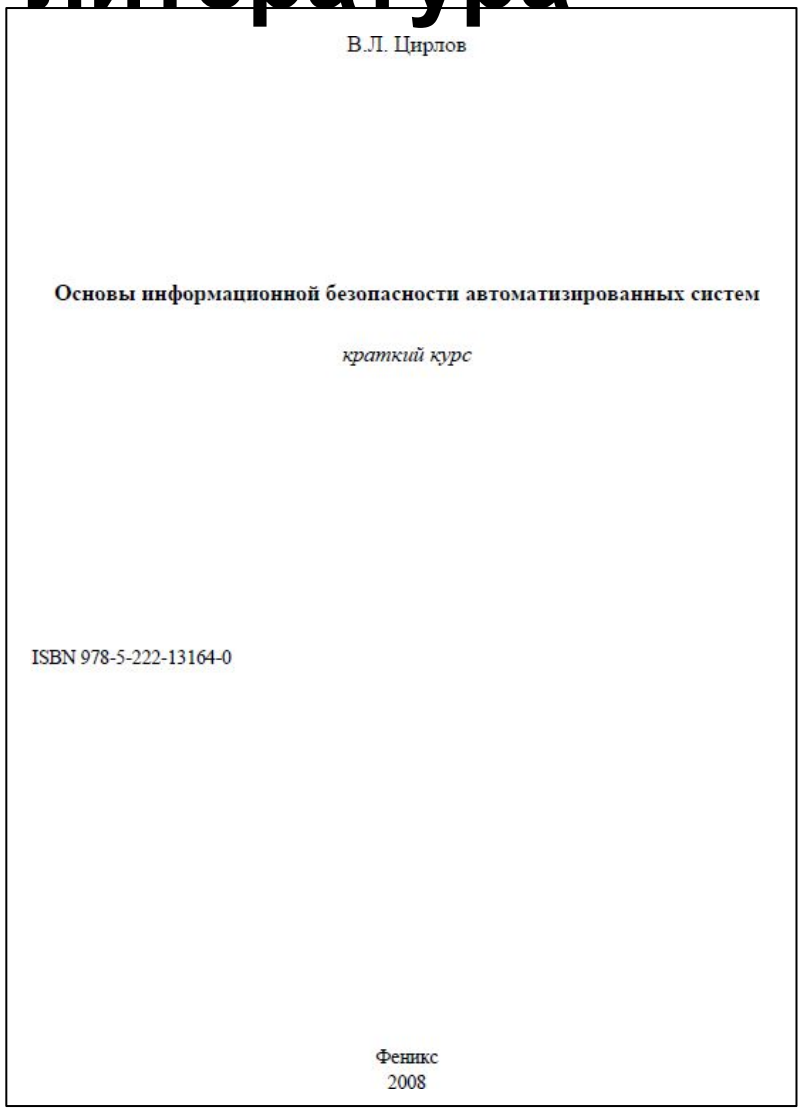
Рекомендуемая литература по теме

Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА- М, 2021. — 336 с. — (Высшее образование).

DOI: https://doi.org/10.29039/1761-6.

ISBN 978-5-369-01761-6.

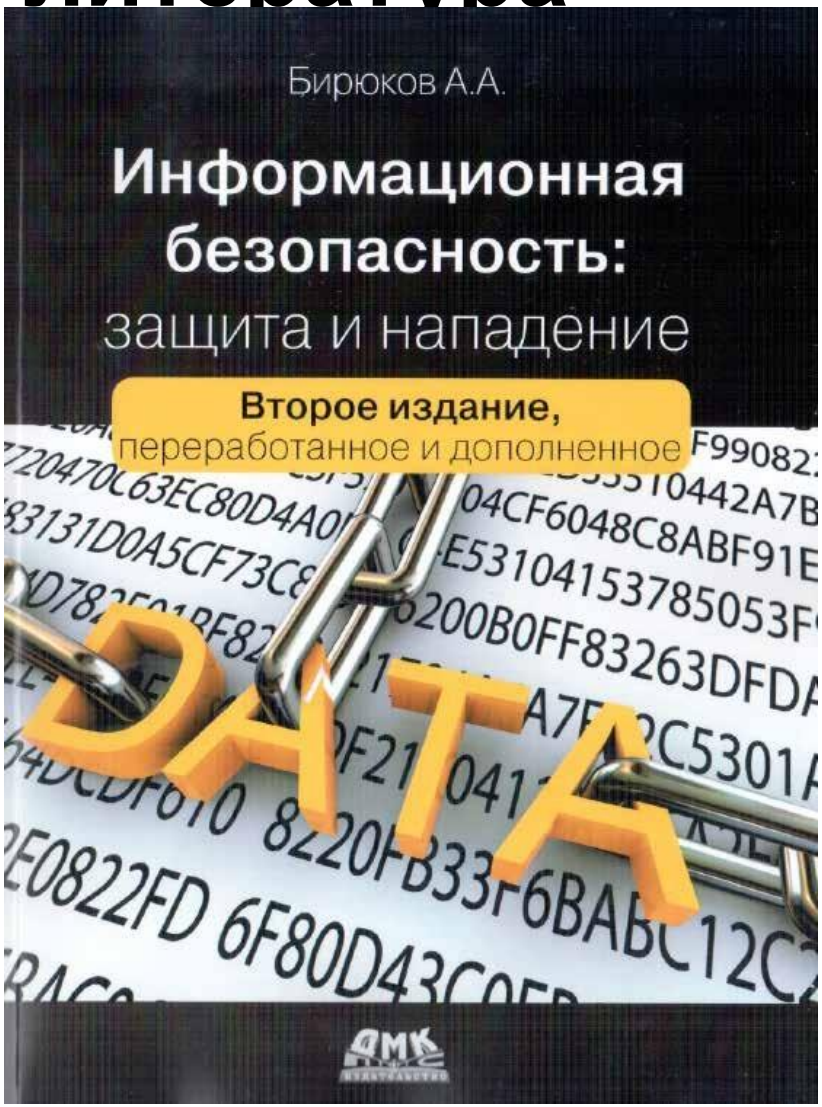
Рекомендуемая литература



Цирлов В. Л. Основы информационной безопасности: краткий курс / В.Л. Цирлов.– Ростов н/Д: Феникс, 2008. – 253 с.

https://www.e-reading.life/bookreader.php/134422/Osnovy_informacionnoii_bezopasnosti._Kratkiii_kurs.pdf

Рекомендуемая литература



Бирюков А. А.

Информационная безопасность: защита и нападение. - Москва: ДМК Пресс, 2017. - 434 с.:

ISBN 978-5-97060-435-9

https://nnmclub.to/forum/viewtopic.php?t=1114555

Дополнительные источники информации по теме методов и средств защиты информации

Telegram каналы

- https://t.me/SecLabNews - Новости ведущего портала по информационной безопасности SecurityLab.ru
- https://t.me/alukatsky - Трансляция блога и Твиттера Алексея Лукацкого, а еще репосты из Телеграмма и публикация уникальных материалов по Информационной Безопасности
- https://t.me/TG_security - IT&Безопасность. Многое о безопасности в интернете и не только.
- https://t.me/singlesecurity - Cyber Security. Канал о кибербезопасности в целом – уязвимости в смартфонах и сервисах, лайфхаки по настройкам приватности в браузере, новое Интернет-законодательство.

Telegram каналы

- https://t.me/news_infosecurity - ИБшнику. Площадка актуальных новостей и событий в сфере информационной безопасност
- https://t.me/searchinform - SearchInform. Информационная безопасность как она есть. Новости и тенденции отрасли. Разбор инцидентов. Практика, экспертный опыт и кейсы реальные
- https://t.me/NeKaspersky - НеКасперский.Канал про адекватное восприятие того, что происходит в кибербезопасности вне политического мире IT и дискурса.
- https://t.me/alexmakus - Информация опасносте. Новости о безопасности, угрозах, атаках и т.д.
- https://t.me/true_secator - Secator. Канал делает обзоры на хакерские группировки, пишет про году атаки вирусов-участившиеся в этом вымогателей

1.1 Основные понятия и терминология информационной безопасности

Термины и определения

- Под **информацией** будем понимать сведения о лицах, предметах, фактах, событиях, явлениях и процессах. Информация может существовать в виде бумажного документа, физических полей и сигналов (электромагнитных, акустических, тепловых и т.д.), биологических полей (память человека) и в других видах.
- В дальнейшем будем рассматривать информацию в документированной (на бумаге, диске и т. д.) форме и в форме физических полей (радиосигналы, акустические сигналы и т.д.).

- **Информация** – это сведения (сообщения, данные) независимо от формы их представления.

Термины и определения

- **Информационный объект** - среда, в которой информация создается, передается, обрабатывается или хранится.

- **Защита информации** — деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

Термины и определения

- **Безопасность информации (данных)** — состояние защищенности информации (данных), при котором обеспечиваются ее (их) конфиденциальность, доступность и целостность.
- **Безопасность информации (данных)** определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые при применении информационной технологии

Термины и определения

- **Конфиденциальность информации** — состояние информации (ресурсов автоматизированной информационной системы), при котором доступ к ней (к ним) осуществляют только субъекты, имеющие на него право.

- **Целостность информации** — состояние информации (ресурсов автоматизированной информационной системы), при котором изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Термины и определения

- **Доступность информации** — состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно... К правам доступа относятся: право на чтение, изменение, копирование, уничтожение информации, а также право на использование, уничтожение ресурсов.

- **Защищаемая информация** — информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Термины и определения

- **Нарушение конфиденциальности** — нарушение свойства информации быть известной только определенным субъектам.

- **Нарушение целостности** — несанкционированное изменение, искажение, уничтожение информации.

- **Нарушение доступности** (отказ в обслуживании) — нарушаются доступ к информации, работоспособность объекта, доступ в который получил злоумышленник.

Термины и определения

- Под **угрозой** информационной безопасности объекта будем понимать возможные воздействия на него, приводящие к ущербу.

- Некоторое свойство объекта, делающее возможным возникновение и реализацию угрозы, будем называть **уязвимостью**.

- Действие злоумышленника, заключающееся в поиске и использовании той или иной уязвимости, будем называть **атакой**.

Термины и определения

- **Защита информации от утечки** – защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на предотвращение (затруднение) получения защищаемой информации (иностранными) разведками и другими заинтересованными субъектами.

Термины и определения

- **Носитель защищаемой информации** — физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.
- **Защита информации от разглашения** — защита информации от несанкционированного ознакомления (потребителей), информации.

Термины и определения

- **Вторжение (атака)** – действие, целью которого является осуществление несанкционированного доступа к информационным ресурсам.

- **Компьютерная атака** – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы

Термины и определения

- **Инцидент информационной безопасности** – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

- Примечание.
  Инцидентами информационной безопасности являются:
  1. утрата услуг, оборудования или устройств;
  2. системные сбои или перегрузки;
  3. ошибки пользователей;
  4. несоблюдение политики или рекомендаций по ИБ;
  5. нарушение физических мер защиты;
  6. неконтролируемые изменения систем;
  7. сбои программного обеспечения и отказы технических средств;

Термины и определения

- **Утечка информации** – неконтролируемое распространение информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации иностранными разведками.

- **Канал утечки информации** – способ утечки информации; предполагает сценарий, в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность.

Термины и определения

- **Защищенный информационный объект** — это объект со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.
- **Комплексная защита ИО** — совокупность методов и средств (правовых, организационных, физических, технических, программных).
- **Политика безопасности** — совокупность норм, рекомендаций, регламентирующих работу, правил, средств защиты ИО от заданного множества угроз безопасност и.

Термины и определения

- **Умышленная утечка информации (злонамеренная)** такая утечка, когда пользователь, работающий с информацией ограниченного доступа, предполагая возможные негативные последствия своих действий, осознавая и противоправны характе бы предупрежден об ответственности и действовал из корыстных побуждений, преследуя личную выгоду, или руководствовался иными мотивами (месть, зависть, личная неприязнь и т.д.).
- При этом в результате таких действий контроль над информацией со стороны ее обладателя был утрачен. При этом неважно, повлекли ли действия пользователя негативные последствия в действительности, равно как и то, понесла ли компания убытки, связанные с действиями пользователя. К умышленным утечкам также относятся все утечки, спровоцированные хакерскими атаками или физическим доступом извне к носителям информации ограниченного доступа, принадлежащей компании.

Каналы утечки информации

- На данный момент выделяют 8 самостоятельных каналов утечки (далее - классификаторы):

1. **Оборудование (сервер, СХД, ноутбук, ПК)**, – компрометация информации в ходе обслуживания, в результате кражи или потери оборудования.
2. **Мобильные устройства** – утечка вследствие нелегитимного использования мобильного устройства/кражи мобильного устройства (смартфоны, планшеты). Использование данных устройств рассматривается в рамках парадигмы BYOD.
3. **Съемные носители** – потеря/кража съемных носителей (CD, DVD, USB, карты памяти и др.).

Каналы утечки информации

- На данный момент выделяют 8 самостоятельных каналов утечки (далее - классификаторы):

4. **Сеть (сетевой канал)** – утечка через браузер (отправка данных через вебинтерфейс в личную почту, формы ввода в браузере), нелегитимное использование внутренних ресурсов сети, FTP, облачных сервисов, нелегитимная публикация информации на веб-сервисе.
5. **Электронная почта** – утечка данных через корпоративную электронную почту.
6. **Бумажные документы** – утечка информации на бумаге) вследствие неправильного хранения/утилизации бумажной документации, через печатающие устройства (отправка

та печать и кража/вынос конфиденциальной информации

Каналы утечки информации

- На данный момент выделяют 8 самостоятельных каналов утечки (далее - классификаторы):

7. **IM–сервисы мгновенных сообщений** – утечка информации при передаче ее голосом, в текстовом виде, а также через видео - при использовании мессенджеров.
8. **Не определено** – категория, используемая в случае, когда сообщение об инциденте в СМИ не позволяет точно определить канал утечки.

Особенности современных ИБ

- **Особенностями современных информационных систем являются:**

1. усложнение программных и аппаратных средств информационных систем;
2. рост числа автоматизированных процессов в системах обработки информации и важности принимаемых на их основе решений;
3. территориальная удаленность различных компонентов информационных систем и передача важной информации между ними;
4. подключение к ресурсам информационных систем большого количества пользователей различных категорий с различными правами доступа;
5. накопление и длительное хранение больших массивов данных на электронных носителях в информационных системах;
6. объединение в единую базу данных информации и различной направленности ресурсов информационных систем;
7. увеличение стоимости программных и аппаратных устройств.

Цель и объект защиты информации

- **Цель защиты информации** — заранее намеченный результат защиты информации. Результатом защиты информации может быть предотвращение ущерба обладателю информации из- за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

- **Объект защиты информации** — информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

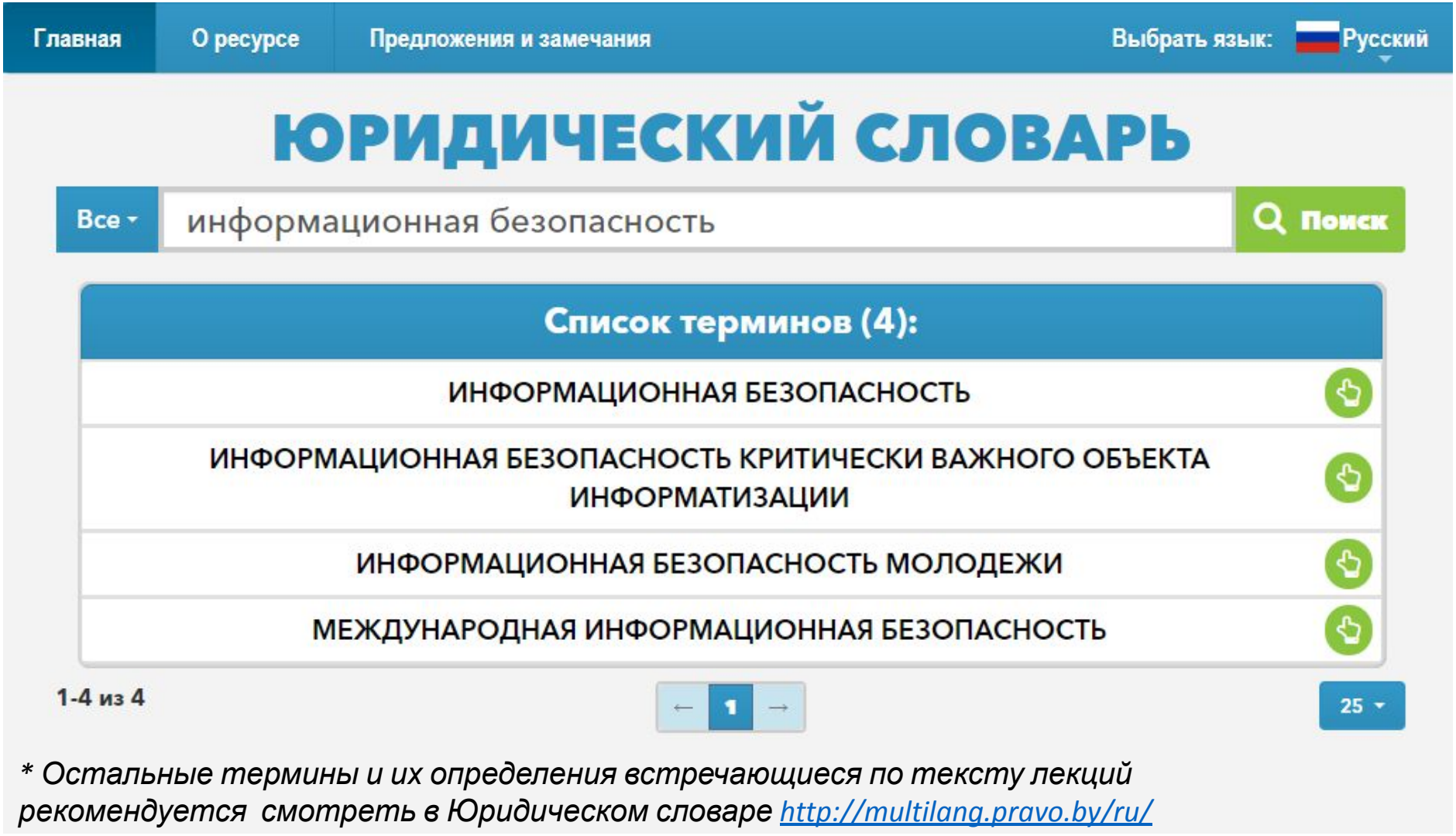
Объекты защиты информации

- **Объектами защиты информации могут быть:**

1. **базы данных.** Угроза может быть связана с несанкционированным доступом к ним, компрометацией конфиденциальных данных, удалением или модификацией данных;
2. **программы.** Угроза может быть связана с внедрением в информационную систему вредоносного программного обеспечения;
3. **технические средства.** Угрозы могут быть связаны с возможностью вывода из строя компьютерной техники в связи со случайными или преднамеренными действиями пользователей или злоумышленников;
4. **персонал.** Угроза может быть связана с созданием злоумышленниками условий, вынуждающих сотрудников предоставить им допуск к конфиденциальной информации (удержание в заложниках, шантаж, подкуп и т. д.).

Юридический словарь

http://multilang.pravo.by/ru/



** Остальные термины и их определения встречающиеся по тексту лекций рекомендуется смотреть в Юридическом словаре http://multilang.pravo.by/ru/*

1.2 Задачи в сфере обеспечения информационной безопасности

Основная задача ИБ

- **Основная задача информационной безопасности** – сбалансированная защита конфиденциальности, целостности и доступности данных, с учетом целесообразности применения и без какого-либо ущерба производительности организации.
- Это достигается, в основном, посредством многоэтапного процесса управления рисками, который позволяет идентифицировать основные средства и нематериальные активы, источники угроз, уязвимости, потенциальную степень воздействия и возможности управления рисками.

Задачи ИБ

https://

КОНЦЕПЦИЯ информационной безопасности

Информация *– это сведения (сообщения, данные) независимо от формы их представления.*

1.3 Виды информации

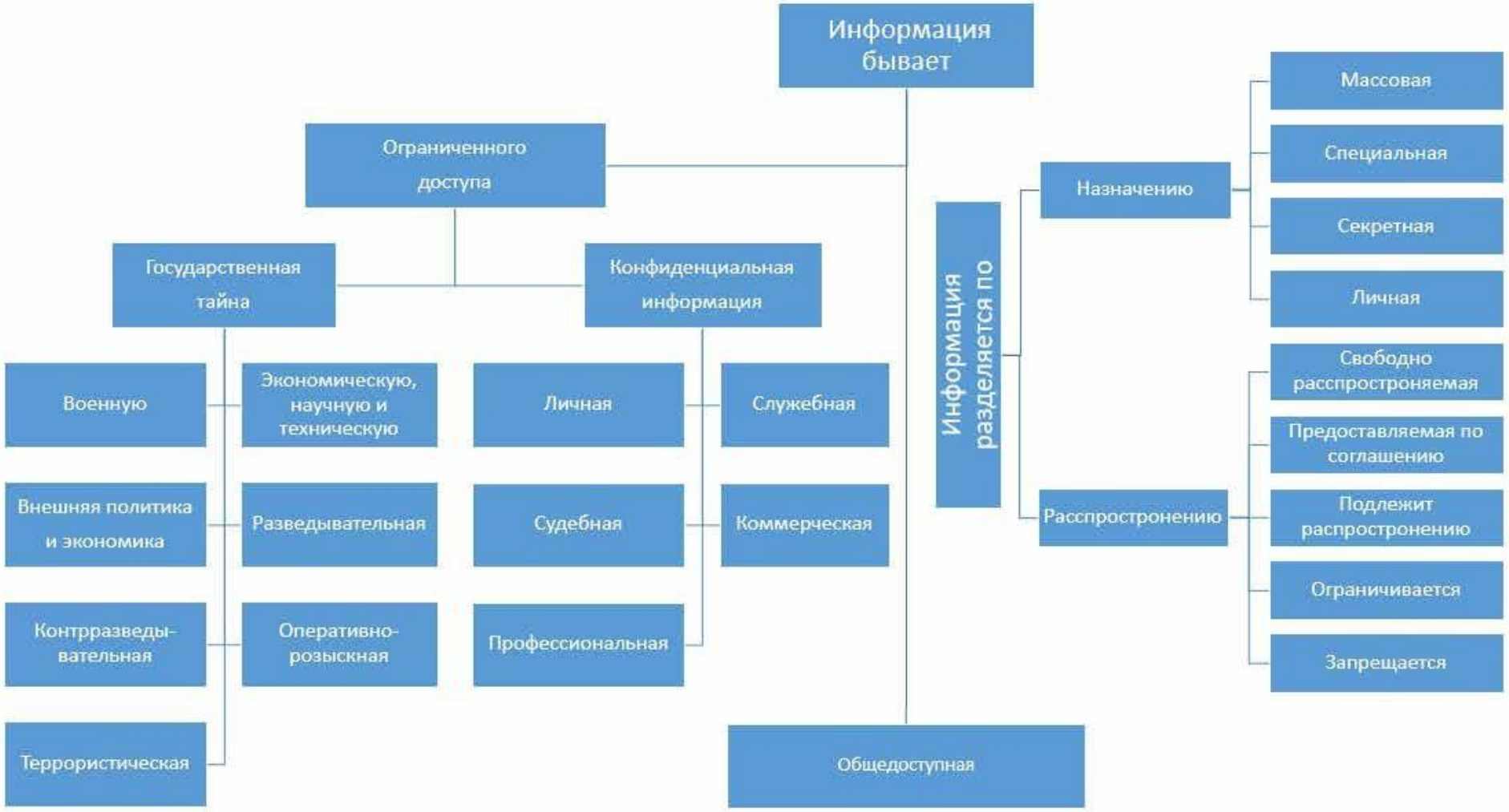
Информация в зависимости от порядка ее предоставления или распространения

- **Информация в зависимости от порядка ее предоставления** или распространения подразделяется на информацию:
  - **Свободно распространяемую**
  - **Предоставляемую по соглашению лиц**, участвующих в соответствующих отношениях
  - Которая в соответствии с законами **подлежит предоставлению или распространению**
  - Распространение, которой в государстве **ограничивается или запрещается**

Виды информации

- Информация по назначению бывает следующих видов:
  - **Массовая** — содержит тривиальные сведения и оперирует набором понятий, понятным большей части социума.
  - **Специальная** — содержит специфический набор понятий, которые могут быть не понятны основной массе социума, но необходимы и понятны в рамках узкой социальной группы, где используется данная информация.
  - **Секретная** — доступ, к которой предоставляется узкому кругу лиц и по закрытым (защищённым) каналам.

Классификация видов информации



Виды информации

- **Общедоступная информация**.

  К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

- **Информация ограниченного доступа.**

  Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны

Виды информации ограниченного доступа

РБ. Государственная тайна

- **Государственные секреты** подразделяются на две категории: государственную тайну (сведения, составляющие государственную тайну) и служебную тайну (сведения, составляющие служебную тайну).
- **Государственная тайна – сведения, в результате разглашения или утраты которых могут наступить тяжкие последствия для национальной безопасности**
- **Служебная тайна** – сведения, в результате разглашения или утраты которых может быть причинен существенный вред национальной безопасности.
- Служебная тайна может являться составной частью государственной тайны, не раскрывая ее в целом.

РФ. Государственная тайна

- Государственная тайна. Определение государственной тайны содержится в Законе РФ от 21.07.1993 № 5485-1 «О государственной тайне».
- **Государственная тайна** — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, оперативно-розыскной деятельности, контрразведывательной и распространение которых может нанести ущерб безопасности Российской Федерации».
- Для отнесения информации к сведениям, составляющим государственную тайну, в дополнение к Закону «О государственной тайне» принят Указом Президента РФ от 30.11.1995 № 1203 и постоянно обновляемый. «Перечень сведений, отнесенных к государственной тайне», утвержденный
  - В целях борьбы с разглашением государственной тайны установлен определенный порядок пользования сведениями, составляющими государственную тайну, за нарушение установленного порядка виновные привлекаются к уголовной ответственности.

Конфиденциальная информация

- **Конфиденциальность информации** — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

1.4 Информационные системы. Классификация

Информационная система: *Совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств.*

СТБ 34.101.30-2017

СТБ 34.101.30-2017

Информационные технологии. Методы и средства безопасности. Информационные Системы. Классификация

Настоящий стандарт устанавливает классификацию информационных систе

Настоящий стандарт распространяется на информационные системы

Настоящий стандар обеспечива единый методологический подход к классификац информационн систе с учето вид и их обрабатываем информации и м м а организации на них ой процесс вычислительного а.

СТБ 34.101.30-2017 Информационные технологии. Методы и средства безопасности. Информационные Системы. Классификация

- Отнесение информационных систем к классам типовых информационных систем осуществляется на основании:
  - категории доступа обрабатываемой информации;
  - наличия подключения к открытым каналам передачи данных.

СТБ 34.101.30-2017 Информационные технологии. Методы и средства безопасности. Информационные Системы. Классификация

- **В зависимости от категории доступа** обрабатываемой информации устанавливаются четыре группы информационных систем:
  - **группа информационных систем, обрабатывающих информацию, доступ к которой, распространение и (или) предоставление которой не ограничены** в соответствии с Законом «Обинформации, информатизации и защите информации» от 10 ноября 2008 г. № 455-3 (далее - общедоступная информация);
  - **группа информационных систем, обрабатывающих информацию, доступ к которой, распространение и (или) предоставление ограничены** в соответствии с Законом «Обинформации, информатизации и защите информации» от 10 ноября 2008 г. № 455-3 и не содержащую государственных секретов в соответствии с Законом «О государственных секретах» от 19 июля 2010 г. № 170-3 (далее - информация, распространение и (или) предоставление которой ограничено);
  - **группа информационных систем, обрабатывающих информацию в соответствии** с Законом «О государственных секретах» от 19 июля 2010 г. №170-3 (далее - С).

- **группа информационных систем, обрабатывающих информацию в соответствии** с Указом Президента «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации» от 25 октября 2011 г. № 486 «Об утверждении Положения о порядке создания, эксплуатации, развития, модернизации и обеспечения безопасной эксплуатации и надежного функционирования критически важных объектов информатизации» от 30 марта 2012 г. № 293 (далее - КВОИ);

СТБ 34.101.30-2017 Информационные технологии. Методы и средства безопасности. Информационные Системы. Классификация

- В зависимости **от наличия подключения к открытым каналам передачи данных** устанавливаются следующие подгруппы информационных систем:
  - подгруппа информационных систем, которые не имеют физических подключений к открытым каналам передачи данных (далее - изолированная);
  - подгруппа информационных систем, которые имеют физические подключения к открытым каналам передачи данных (далее - открытая).

Категории типовых информационных систем по СТБ 34.101.30-2017

- Категории типовых информационных систем, обрабатывающих общедоступную информацию:
  - **категория информационных систем, создаваемых и (или) приобретаемых за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов**, а также средств государственных юридических лиц (далее - **гос**);
  - категория информационных систем, создаваемых и (или) приобретаемых **не за счет средств** республиканского или местных бюджетов, государственных внебюджетных фондов, а также не за счет средств государственных юридических лиц (далее - **частн**).

Категории типовых информационных систем по СТБ 34.101.30-2017

- **Категории типовых информационных систем, обрабатывающих информацию, распространение и (или) предоставление которой ограничено:**
  - категория обрабатывающих (далее - **фл**) информационных следующую информацию
  - категория обрабатывающих (далее - **юл**) информационных следующую информацию

Категории типовых информационных систем по СТБ 34.101.30-2017

- **Категории типовых информационных систем, обрабатывающих информацию, распространение и (или) предоставление которой ограничено:**
  - категория информационных систем, обрабатывающих следующую информацию (далее - **фл**)
  - категория информационных систем, обрабатывающих следующую информацию (далее - **юл**)
  - категория информационных систем, обрабатывающих сведения, содержащиеся в Перечне сведений, относящихся к служебной информации ограниченного распространения, утвержденном Постановлением Совета Министров

Категории типовых информационных систем по СТБ 34.101.30-2017

- **Категории типовых информационных систем, обрабатывающих информацию, распространение и (или) предоставление которой ограничено:**
- **категория информационных систем, обрабатывающих следующую информацию (далее - фл):**
- **1)** сведения, однозначно идентифицирующие физическое лицо (персональные данные);
- **2)** сведения о факте обращения пациента за медицинской помощью и состоянии его здоровья, сведения о наличии заболевания, диагнозе, возможных методах оказания медицинской помощи, рисках, связанных с медицинским вмешательством, а также о возможных альтернатив предлагаемому медицинскому вмешательству, иные сведения, в том числе личного характера, полученные при оказании пациенту медицинской помощи, а в случае смерти - и информация о результатах патологоанатомического исследования (врачебная тайна) в соответствии с Законом Республики Беларусь «О здравоохранении» от 18 июня 1993 г. № 2435-XII;
- **3)** сведения о счетах и вкладах (депозитах) физических лиц, в том числе о наличии счета в банке (небанковской кредитно-финансовой организации), его владельце, номере и других реквизитах счета, размере средств, находящихся на счетах и во вкладах (депозитах), а равно сведения о конкретных сделках, об операциях без открытия счета, операциях по

Категории типовых информационных систем по СТБ 34.101.30-2017

- **Категории типовых информационных систем, которой ограничен доступ к информацию, распространение и (или) предоставление обрабатывающих**
- **Категория информационных систем, обрабатывающ их следующу ю информацию (далее - фл):**
- **4)** сведения о физических лицах, полученные органами, указанными в Налоговом Кодексе Республики Беларусь, о плательщиках (иных лицах) (налоговая тайна);
- **5)** сведения о вопросах, по которым клиент обратился за юридической помощью, суть консультаций, разъяснений, справок, полученных клиентом от адвоката, сведения о личной жизни клиента, информация, полученная от клиента, об обстоятельствах совершения преступления по уголовному делу, по которому адвокат осуществлял защиту прав, свобод и интересов клиента, а также сведения, составляющие коммерческую тайну клиента (адвокатская тайна) в соответствии с Законом РБ «Об адвокатуре и адвокатской деятельности в Республике Беларусь» от 30 декабря 2011 г. № 334-3;
- **6)** сведения об исключительном праве (интеллектуальной собственности) физического лица на охраняемые результаты интеллектуальной деятельност
- **7)** иные сведения о частной жизни физического лица, доступ к которой ограничен законодательными актами Республики Беларусь;

Категории типовых информационных систем по СТБ 34.101.30-2017

- **Категории типовых информационных систем, обрабатывающих информацию, распространение и (или) предоставление которой ограничено:**
- **- категория информационных систем, обрабатывающих следующую информацию (далее - юл):**
- **1)** сведения, которые имеют коммерческую ценность для их обладателя в силу неизвестности
  третьим лицам (коммерческая тайна) в соответствии с Законом РБ «О коммерческой тайне» от 5
  января 2013 г. № 16-З;
- **2)** сведения о счетах и вкладах (депозитах) юридических лиц, в том числе о наличии счета в банке (небанковской кредитно-финансовой организации), его владельце, номере и других реквизитах счета, размере средств, находящихся на счетах и во вкладах (депозитах), а равно сведения о конкретных сделках, об операциях без открытия счета, операциях по счетам и
  вкладам (депозитам), а также об имуществе, находящемся на хранении в банке (банковская тайна) в соответствии с Банковским кодексом РБ;
- **3)** сведения о юридических лицах, полученные органами, указанными в Налоговом кодексе РБ, о плательщиках (иных обязанных лицах) (налоговая тайна);
- **4)** сведения об объектах, в отношении которых исключительные права на результаты интеллектуальной деятельности принадлежат Республике Беларусь;
- **5)** информация, содержащаяся в делах об административных правонарушениях, материалах и
  уголовных делах органов уголовного преследования и суда до завершения производства по делу
  в соответствии с Процессуально-исполнительным кодексом РБ «Об административных правонарушениях» от 20 декабря 2006 г. № 194-З и Уголовно-процессуальным кодексом

Классификация информационных систем по СТБ 34.101.30-2017

- **На основании групп, подгрупп и категорий типовых информационных систем: устанавливаются следующие классы**
- **класс 6-частн** - совокупность негосударственных информационных систем, которые обрабатывают общедоступную информацию и не имеют подключений к открытым каналам передачи данных;
- **класс 6-гос** - совокупность государственн информационных систем, которые обрабатывают их общедоступную информацию и не имеют подключений к открытым каналам передачи данных;
- **класс 5-частн** - совокупность негосударственных информационных систем, которые обрабатывают общедоступную информацию и подключены к открытым каналам передачи данных;

Классификация информационных систем по СТБ 34.101.30-2017

- **класс 5-гос** - совокупность государственных информационн систем, которые обрабатывают общедоступную информацию и подключены к ых каналам передачи открытым данных;
- **класс 4-фл** - совокупность систе информационных м, которые обрабатывают информацию, распространение и (или) предоставление которой ограничено затрагивающую интересы физического лица), и информацию, подключений к открытым каналам передачи не имеют данных;
- **класс 4-юл** - информационн систе совокупность м, которые обрабатывают информацию, распространение и (или) предоставление которой ограничено ых затрагивающую безопаснос организаци информацию, з исключением сведений, составляющих ю государственные секреты и служебной информации ограниченного , а распространения), и не имеют подключений к открытым каналам передачи данных;

Классификация информационных систем по СТБ 34.101.30-2017

- **класс 4-дсп** - информационные системы, которые обрабатывают служебную информацию ограниченного распространения и не имеют подключений к открытым каналам передачи данных;
- **класс 3-фл** - информационные системы, которые обрабатывают информацию, распространение и (или) предоставление которой ограничено затрагивающую интересы физического лица), и подключены к открытым каналам передачи данных;
- **класс 3-юл** - информационные системы, которые обрабатывают информацию, распространение и (или) предоставление которой ограничено затрагивающую безопасность организации (за исключением сведений, составляющих государственные секреты и служебной информации ограниченного распространения), и подключены к открытым каналам передачи данных;

Классификация информационных систем по СТБ 34.101.30-2017

- **класс3-дсп** - совокупность информационных систем, которые обрабатывают служебную информацию ограниченного распространения и подключены к каналам передачи данных;
- **класс 2** - совокупность информационныхсистем, которые соответствуют критериям и показателям ущерба, установленным Постановлением Совета Министров РБ «О некоторых вопросах безопасной эксплуатации и функционирования критически важных объектов информатизации» от 30 марта 2012 г. № 293;
- **класс 1** - совокупность информационных систем, которые обрабатывают информацию в соответствии с Законом Республики Беларусь «О государственных секретах» от 19 июля 2010 г. № 170-З.

Классификация информационных систем по СТБ 34.101.30-2017

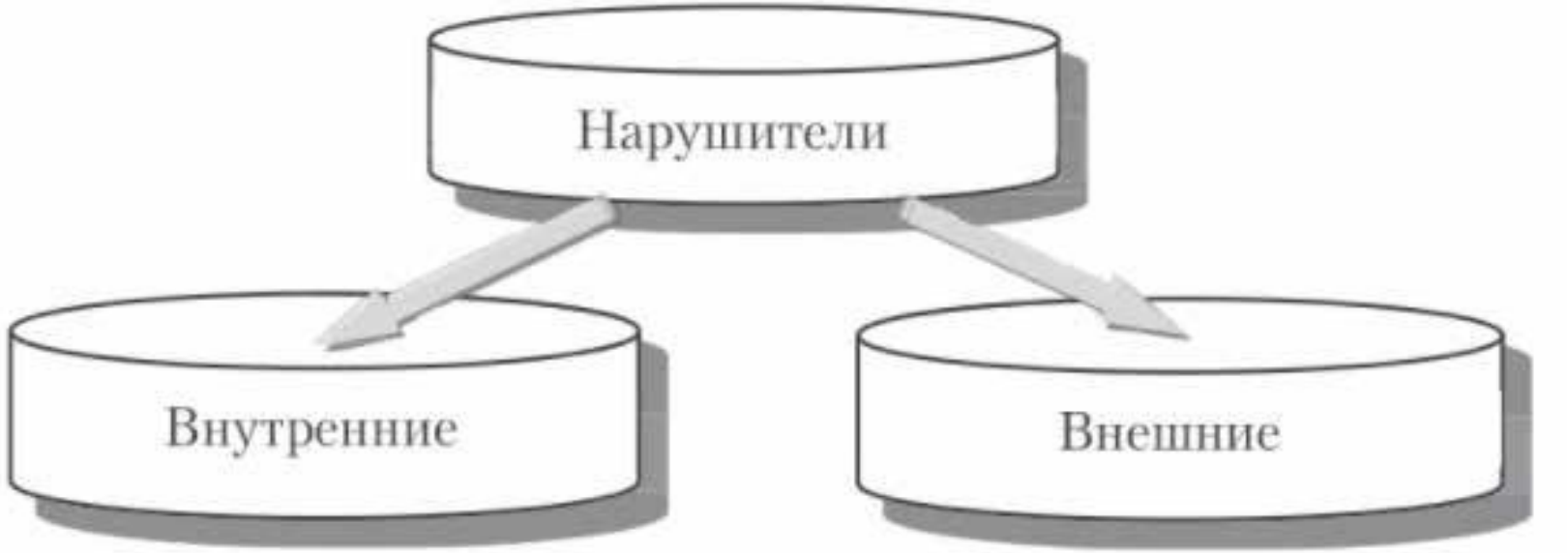
- **Для информационных систем, которые могут быть отнесены к нескольким классам, присвоение класса заполняется перечислением классов, к которым они могут быть отнесены.**
- **Примеры.** Информационной системе, в которой обрабатывается информация, распространение и (или) предоставление которой ограничено затрагивающие интересы юридических (за исключением сведений, составляющих государственные секреты, и информации ограниченного распространения) и физических лиц, будут присвоены классы 3-фл, 3-юл.
- Схема разбиения на классы представлена в таблице

Группа	Общедоступная информация				Информация, распространение и (или) предоставление которой ограничено						КВОИ	С
Подгруппа	Изолированная		Открытая		Изолированная			Открытая			–	–
Категория	частн	гос	частн	гос	фл	юл	дсп	фл	юл	дсп	–	–
Класс	6-частн	6-гос	5-частн	5-гос	4-фл	4-юл	4-дсп	3-фл	3-юл	3-дсп	2	1

1.5 Нарушители информационной безопасности

Нарушители

- Утечка конфиденциальной информации становится возможной в результате нарушений конфиденциальным режима работы с информацией сотрудникам компании или противоправных действий злоумышленников.



Внутренние нарушители

- **Внутренними нарушителями (инсайдерами)** информационной безопасности могут быть следующие категории сотрудников:
  - обслуживающий здание персонал (уборщицы, электрики, сантехники и др.);
  - персонал, обслуживающий технические средства здания (системы кондиционирования, вентиляции, отопления и др.);
  - пользователи информационной системы;
  - сотрудники отделов разработки и сопровождения ПО;
  - системные администраторы;
  - сотрудники отдела информационной безопасности;
  - руководители различных уровней.

Внешние нарушители

- Внешними нарушителями информационной безопасности могут быть:
  - клиенты, посетители, представители других организаций;
  - представители конкурирующих организаций или лица, действующие по их заданию;
  - лица, умышленно нарушившие пропускной режим;
  - лица, случайно находящиеся на контролируемой территории.

Характеристики и возможности нарушителей информационной безопасности

Объекты компании	Характеристика нарушителя	Возможности нарушителя
Территория объекта вне зданий, телекоммуникации	Лица, имеющие доступ на территорию объекта, но не имеющие доступ в здания и помещения	Имеют доступ к линиям связи, выходящим за пределы здания. Перехват данных по техническим каналам
Здания объекта, телекоммуникации	Лица, имеющие доступ на территорию, в здания, но не имеющие доступ в служебные помещения	Имеют информацию о размещении поста охраны, системе видеонаблюдения
Представительские помещения, комнаты для переговоров	Лица, у которых есть доступ в представительские помещения и комнаты для переговоров, но нет доступа в служебные помещения	Имеют информацию о порядке пропуска, расположении помещений, системе видеонаблюдения

Характеристики и возможности нарушителей информационной безоп

Объекты компании	Характеристика нарушителя	Возможности нарушителя
Помещения пользователей и администраторов ИС	1. Зарегистрированные пользователи, имеющие ограниченный доступ к ресурсам. 2. Зарегистрированные пользователи, имеющие удаленный доступ к ИС. 3. Зарегистрированные пользователи с правами системного администратора. 4. Зарегистрированные пользователи с правами администратора безопасности ИС. 5. Программисты — разработчики ПО	1. Имеют доступ к части ресурсов. Имеют часть данных о топологии ИС. Могут установить программно-аппаратные закладки. 2. Имеют данные о топологии ИС, физический доступ к элементам сети. 3. Имеют всю информацию об ИС, полный доступ. 4. Имеют доступ к методам и средствам защиты ИС. 5. Имеют данные о ПО, могут вносить изменения в ПО ИС

Характеристики и возможности нарушителей информационной безопасности

Объекты компании	Характеристика нарушителя	Возможности нарушителя
Серверные помещения	1. Зарегистрированные пользователи с правами администратора безопасности. 2. Зарегистрированные пользователи с правами системного администратора	1. Имеют доступ к настройке сети. 2. Имеют доступ к конфигурации ИС

Мотивы нарушений информационной безопасности

Классификация нарушителей ИБ

- **Нарушителей ИБ можно классифицировать следующим образом.**

1. По уровню знаний об информационной системе
2. По уровню возможностей (используемым методам и средствам).
3. По времени действия.
4. По месту действия.

Классификация нарушителей ИБ

По уровню знаний об информационной системе

- **По уровню знаний об информационной системе:**
  - знает функциональные особенности информационной системы, основные закономерности формирования в ней массивов данных и потоков запросов к ним, умеет пользоваться штатными средствами ИС;
  - обладает высоким уровнем знаний и опытом эксплуатации технических средств;
  - обладает высоким уровнем знаний в области программирования и компьютерной техники, в вопросах проектирования и эксплуатации информационной системы;
  - знает структуру, функции и механизмы действия средств защиты информационной системы, их недостатки

Классификация нарушителей ИБ

По уровню возможностей (используемым методам и средствам)

По уровню возможностей (используемым методам и средствам)

- **По уровню возможностей (используемым методам и средствам).**
  - применяющий агентурные методы получения сведений;
  - применяющий пассивные средства (технические средства перехвата без модификации компонентов системы);
  - использующий только штатные средства и недостатки систем защиты (несанкционированные действия с использованием разрешенных средств), а также компактные съемные носители информации, которые могут скрытно проноситься через посты охраны;
  - применяющий методы и средства активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных

Классификация нарушителей ИБ

По времени действия

- **По времени действия.**
  - в процессе функционирования информационной системы;
  - в период неактивности компонентов системы (в нерабочее время, во время плановых перерывов в ее работе для обслуживания и ремонта и т.п.);
  - в любом случае.

Классификация нарушителей ИБ

По месту действия

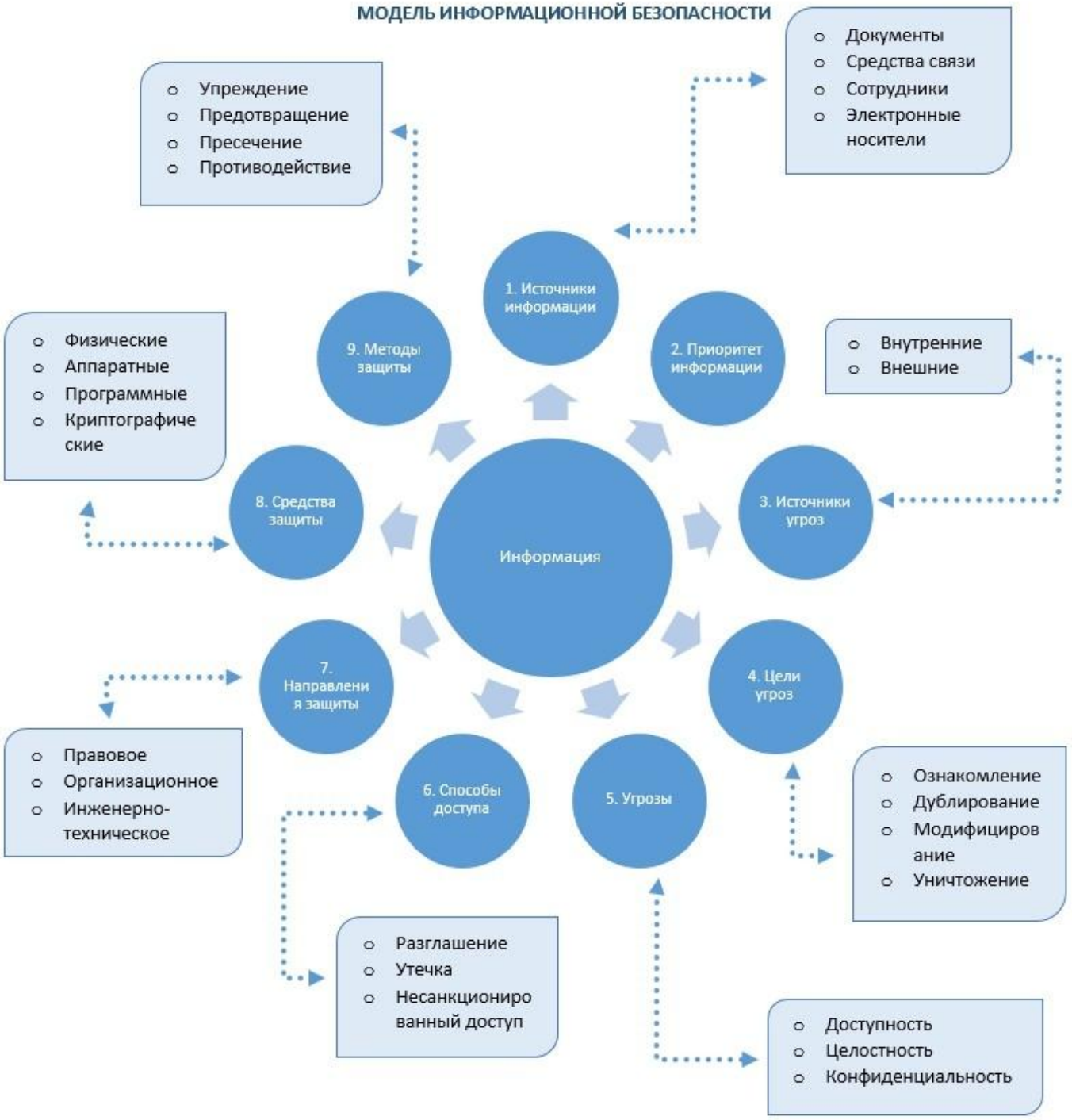
- **По месту действия.**
  - без доступа на контролируемую территорию компании;
  - с контролируемой территории без доступа в здания и сооружения;
  - из зданий без доступа в помещения;
  - внутри помещений без доступа к информационной системе;
  - с рабочих мест пользователей (операторов) информационной системы;
  - с доступом в защищенные зоны информационной системы (базы данных, архивов и т.п.);
  - с доступом в зону управления средствами обеспечения безопасности информационной

1.6 Методы защиты информации

Защита информации

- **Защита информации** представляет собой **принятие правовых, организационных и технических мер**, направленных на:
  - **Обеспечение** защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
  - **Соблюдение** конфиденциальности информации ограниченного доступа;
  - **Реализацию** права на доступ к информации.

Концептуальная модель информационной безопасности



Основные методы об

Основные методы обеспечения ИБ

- **Сервисы сетевой безопасности** представляют собой механизмы защиты информации, обрабатываемой в распределённых вычислительных системах и сетях.
- **Инженерно–технические методы** ставят своей целью обеспечение защиты информации от утечки по техническим каналам – например, за счёт перехвата электромагнитного излучения или речевой информации.
- **Правовые и организационные методы защиты информации** создают нормативную базу для организации различного рода деятельности

Основные методы обеспечения ИБ

- **Теоретические методы обеспечения информационной безопасности** в свою очередь, решают две основных задачи.
- **Первая** из них – это **формализация разного рода процессов, связанных с обеспечением информационной безопасности**. Так например формальные модели управления доступом позволяют строго описать все возможные информационные потоки в системе и, значит, гарантировать выполнение требуемых свойств безопасности.
- Отсюда непосредственно вытекает **вторая задача – строгое обоснование корректности и адекватности функционирования систем обеспечения информационной безопасности** при проведении анализа их защищённости. Такая задача возникает, например, при проведении сертификации автоматизированных систем по требованиям безопасности информации.

Средства защиты информации

- Средства защиты информации принято делить на:
  - нормативные (неформальные)
  - и технические (формальные)

Средства защиты информации

- **Неформальными средствами защиты информации** – являются нормативные (законодательные), административные (организационные) и морально- этические средства, к которым можно отнести: документы, правила, мероприятия.

- **Формальные средства защиты** – это специальные технические средства и программное обеспечение, которые можно разделить на физические, аппаратные, программные и криптографические.

Классификация средства защиты информации

Методы и средства защиты информации

Тема: Основы информационной безопасности, методов и средств защиты информации

Благодарю за внимание

Контрольные вопросы по теме

1. Что такое информация?
2. Что такое защита информации?
3. Что такое компьютерная атака?
4. Что такое инцидент информационной безопасности?
5. Что является инцидентом информационной безопасности?
6. Что такое утечка информации?
7. Что такое политика безопасности?
8. Какие каналы утечки информации вы знаете?
9. Назовите цель защиты информации.

Контрольные вопросы по теме

10. Что может выступать в качестве объектов защиты информации?
11. Назовите основные задачи информационной безопасности.
12. Назовите виды информации.
13. Назовите виды конфиденциальной информации.
14. Что такое государственная тайна
15. Назовите нарушителей информационной безопасности (внутренних и внешних)

Контрольные вопросы по теме

17. Расскажите классификацию нарушителей информационной безопасности.
18. Назовите основные методы обеспечения информационной безопасности.
19. Расскажите укрупненно какие есть средства защиты информации.

Список использованных источников

1. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 201 с. — (Среднее профессиональное образование). - ISBN 978-5-16- 016583-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1191479
2. Цирлов В. Л. Основы информационной безопасности: краткий курс / В.Л. Цирлов.– Ростов н/Д: Феникс, 2008. – 253 с. https://www.e-reading.life/bookreader.php/134422/Osnovy_informacionnoii_bezopasnosti._Kratkiii_kurs.pdf
3. Экспертно-аналитический центр InfoWatch. Утечки информации ограниченного доступа: отчет за 9 месяцев 2020 г. https://d-russia.ru/wp-content/uploads/2020/12/infowatch_2020_9_monts_data_leak.pdf
4. Википедия. Информационная безопасность https://ru.wikipedia.org/wiki/Информационная_безопасность#:~:text=Основная%20задача%20информа_ционной%20безопасности%20—,воздействия%20и%20возможности%20управления%20рисками
5. Постановление Совета Безопасности Республики Беларусь 18.03.2019 № 1 КОНЦЕПЦИЯ информационной безопасности Республики Беларусь https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf
6. Национальный центр правовой информации Республики Беларусь. ЮРИДИЧЕСКИЙ СЛОВАРЬ http://multilang.pravo.by/ru
7. Наименование термина - Защита информации (Национальный центр правовой информации Республики Беларусь) http://multilang.pravo.by/ru/Term/Index/2578?langName=ru&size=25&page=1&type=3
8. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения