Лекция 4. 25/09/2025 г. Неадекватная или Лекция-контрольная №1.

**Замечание. Тот, кто получит и прочитает это письмо до Лекции может потиху начать и продолжить на Лекции!!!!**

***Вопросы в начале Лекции.***

На Лекциях 1, 2, 3 шла речь сами знаете о чём. Так вот для начала проверим, что Вы запомнили или (и) записали. Несколько вопросов. Напоминаю, что на вопросы нужно отвечать ПИСБМЕННО на листочках!!!

4.1. Почему Windows не операционная система. До 8 баллов.

4.2. Почему трояны, «сетевые вирусы», макровирусы», черви не являются «вирусами» до 8 баллов.

4.3. Что такое «Загрузка операционной системы». – до 8 баллов.

Сегодня у Вас будет «сложнейшая лекция». Её не надо будет слушать, параллельно занимаясь не относящимися к курсу БИС делами. Мало того, что её НУЖНО БУДЕТ ЧИТАТЬ и ПИСЬМЕННО ОТВЕЧАТЬ НА НЕХИТРЫЕ ВОПРОСЫ, разбросанные по тексту Лекции, НУЖНО БУДЕТ ДУМАТЬ, АНАЛИЗИРОВАТЬ и ДЕЛАТЬ ВЫВОДЫ. Поэтому ЛИСТОЧКИ, с ответами на вопросы 4.1, 4.2, 4.3 НЕ СДАЁМ В НАЧАЛЕ ЛЕКЦИИ, а ЧИТАЕМ Лекцию 4 и отвечаем ПИСЬМЕННО И РАЗВЁРНУТО на вопросы по тексту Лекции и сдаём написанное в сроки, зашифрованные в конце Лекции. ПИШЕМ ПЕЧАТНЫМИ БУКОВКАМИ, ЧТОБЫ ДЕДУШКА смог прочитать написанное.

Напомню, что результаты написанного будут оцениваться исходя из того, что каждое верно (адекватно) использованное понятие (но не слово) может принести Вам 2 балла, ненаписанное – минус 2 балла, ЧРТ штрафуется как для раба, так и для рабовладельца отрицательным количеством баллов, как и использование помойки.

Напоминаю, что на вопросы нужно отвечать ПИСБМЕННО на листочках!!!

Вопрос 4.4. Возникают ли у Вас какие-либо ассоциации в связи с курсом БИС и событиями со взломом АЭРОФЛОТА летом этого года. Необходимо найти описание возникших проблем и анализ причин, приведших к возможности этого взлома. До 16 баллов.

Как уже было сказано в процессе принуждения Вас к использованию почты mail.ru, и как Вы могли прочувствовать и даже что-то использовать, в рамках этого программного продукта под названием mail.ru (заметьте, что я не говорю, что это какой-то сайт, почта, портал или ещё что-то) появилось нечто (точнее, программный продукт – НЕ «ИИ», НЕ «Нейро-сеть»), позволяющее по тексту, набранному в строке поиска, сгенерировать так называемую ЗАМЕТКУ про чё-нибудь. Вот дедушка так и сделал. Сначала набрал «Безопасность информационных систем» (Именно так и не иначе!!!) и получил следующую ЗАМЕТКУ:

*«Безопасность информационных систем — это неотъемлемая часть успешного функционирования любой организации, предприятия или частного лица. В наше время, когда цифровые технологии проникают во все сферы нашей жизни, вопрос безопасности информационных систем является одним из наиболее важных. В этой статье мы рассмотрим, что такое безопасность информационных систем и как она может быть обеспечена. Безопасность информационных систем — это комплекс мер, направленных на защиту данных и ресурсов от несанкционированного доступа, вредоносных программ и взломов. Она включает в себя множество аспектов, таких как защита информации от утечки, шифрование данных, мониторинг и реагирование на инциденты безопасности, а также обучение и защиту персонала. Одним из ключевых аспектов безопасности информационных систем является защита от вредоносных программ. Это включает в себя защиту от вирусов, троянов, шпионских программ, фишинга и других видов вредоносного ПО. Для этого необходимо использовать антивирусное программное обеспечение, обновлять его и следить за активностью на устройстве. Еще одним важным аспектом безопасности информационных систем является мониторинг и реагирование на инциденты безопасности. Это включает в себя установку и регулярное обновление системы обнаружения вторжений, мониторинг сетевой активности и обнаружение подозрительных действий. Реагирование на инциденты безопасности может быть осуществлено как автоматически, так и вручную, в зависимости от уровня риска. Для обеспечения безопасности информационных систем необходимо также обучать персонал. Внедрение системы обучения в организации может быть полезным для сотрудников в понимании правил безопасности и умении реагировать на потенциальные угрозы. Кроме того, организация должна иметь политику безопасности и контроля доступа к конфиденциальной информации. Наконец, необходимо также понимать, что безопасность информационных систем зависит от того, насколько хорошо защищена сама организация. Резервное копирование данных, регулярное обновление программного обеспечения и создание резервных копий информации — все это важные меры для обеспечения безопасности данных. В целом, безопасность информационных систем является ключевым фактором успешного функционирования организации и предприятия. Она должна быть интегрирована во все аспекты работы и должна быть доступна для постоянного улучшения и контроля».*

Вопрос 4.5. Что такое «фишинг»? Чем он отличается от «Вишинга»?

Мне показалось, что получилось как-то многовато воды, поэтому я «попросил ИИ» сделать заметку по запросу:

«БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»

(именно так – большими буквами), надеясь получить что-то отличное от заметки, запрос на которую был записан маленькими буквами. И мои страхи оправдались – я чуть не подпрыгнул на стуле – почти точно так же, когда один человек меня напугал своим возмущением по поводу mailware. Вот что получил:

**«Безопасность информационных систем является одной из ключевых задач в современном мире, где информация играет решающую роль в экономике, политике и повседневной жизни. Для обеспечения безопасности информационных систем применяются различные методы и технологии, направленные на предотвращение несанкционированного доступа, защиту данных от утечек и минимизацию рисков кибератак. Одним из наиболее эффективных методов защиты является внедрение многофакторной аутентификации. Это процесс, при котором для доступа к информации или ресурсам требуется не только традиционная логин-парольная комбинация, но и дополнительные средства, такие как биометрические данные, одноразовые пароли (OTP) или аппаратные токены. Многофакторная аутентификация значительно снижает вероятность взлома и защищает данные от несанкционированного доступа. Кроме того, важным элементом безопасности является регулярное обновление программного обеспечения и системных компонентов. Обновления устраняют уязвимости, которые могут быть использованы злоумышленниками для проникновения в систему. Также важно проводить регулярные аудиты безопасности и внедрять лучшие практики по защите данных. Также стоит отметить значимость обучения и информирования пользователей о мерах безопасности. Информирование сотрудников о правилах использования личных и корпоративных данных, а также о том, как распознавать и сообщать о подозрительных действиях, помогает снизить риск утечек информации и повысить общую киберграмотность. Таким образом, комплексный подход к безопасности информационных систем, включающий использование многофакторной аутентификации, регулярные обновления, аудит безопасности и обучение пользователей, является ключевым фактором для обеспечения защиты информации и предотвращения кибератак.**

**Вопрос 4.6. Указать хотя бы одно СЛОВО из приведенных выше изысков того, что называется «ИИ» от mail.ru, которое следует отнести к ненормативной лексики курса БИС.**

Нормально?! Понятие одно и то же, а «водичка разная». Что ж это за «ИИ» такой? Или он такой сильно крутой, что адаптируется к конечному пользователю, сидящему за компом и набирающему запросы разными буквами?!

Но и это ещё не всё. Я сделал запрос про «безопасность информационных систем» в следующем виде:

«Безопасность инфосистем». И получил «подарочек из Африки» (даже уже не помню, откуда появилась у меня эта фраза «подарочек из Африки» - надо посмотреть в «ИИ»).

Вопрос 4.7. Используя санкционированно помойку, всемирную липкость найти источник, откуда у дедушки появилась фраза «Подарочек из Африки». Указать этот источник и ссылку на сайт, где этот источник указан.

В наше время информационные технологии играют ключевую роль в жизни каждого человека. Они проникают во все сферы нашей деятельности, от бизнеса до личной жизни, и мы не можем представить себе их функционирование без надежной и безопасной информационной инфраструктуры. Поэтому, обеспечение безопасности информационных систем становится все более важным вопросом. Информационная безопасность - это комплекс мероприятий, направленных на защиту данных и информации от несанкционированного доступа, а также от внешних угроз, таких как вирусы, хакерские атаки, фишинг и т.д. Для обеспечения безопасности информационных систем используются различные методы и технологии, такие как шифрование данных, аутентификация, контроль доступа и резервное копирование. Одним из ключевых элементов информационной безопасности является защита от взлома. Для этого используются различные методы, такие как пароли, шифрование данных и использование средств защиты от вредоносных программ. Кроме того, важно иметь резервные копии данных, которые могут быть использованы для быстрого восстановления системы в случае взлома. Другим важным аспектом информационной безопасности является мониторинг и анализ производительности системы. Это позволяет обнаруживать и устранять уязвимости, которые могут привести к нарушению безопасности. Регулярный мониторинг и анализ производительности системы позволяет обнаруживать и устранять проблемы, которые могут повлиять на безопасность данных. Однако, обеспечение безопасности информационных систем не ограничивается только их защитой от внешних угроз. Важно также следить за внутренним состоянием системы, чтобы минимизировать возможность взлома и других видов атак. Таким образом, обеспечение безопасности информационных систем является неотъемлемой частью нашей современной жизни. Это требует комплексного подхода, который включает в себя множество методов и технологий, а также регулярный мониторинг и анализ производительности системы. Только так можно обеспечить надежную и безопасную работу информационных систем и защитить конфиденциальные данные.

***Вопрос 4.8.*** Выделить и записать на ЛИСТОЧКАХ, ЧТО ОБЪЕДИНЯЕТ ЭТИ ТРИ ЗАМЕТКИ МЕЖДУ СОБОЙ и в ЧЁМ Вы видите ОТЛИЧИЯ. НУЖНО ПО ПУНКТАМ ПЕРЕЧИСЛИТЬ: 1. Что такое БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ. 2. Основные подходы к обеспечению информационных систем, которые упоминаются в каждой из трёх заметок. То есть нужно внимательно прочитать эти три заметки, вспомнить про свою, проанализировать их и ПЕРЕХОДЯ ОТ абстрактного к конкретному, а затем от конкретного к абстрактному, выделить ОБЩЕЕ, ХАРАКТЕРНОЕ ДЛЯ Понятия «Безопасность информационных систем» вне зависимости от того, каким образом набран запрос. За каждую найденную «общность» можно получить от 8 до 16 баллов в зависимости от адекватности.

Замечание. И это я ещё не набирал запрос с ошибками. Например, надо будет попробовать набрать так: <Бизопаснасть инфармационых сестем». Сейчас попробую». Попробовал. И Вы попробуйте и опишите результат в ответе на вопрос 4.9.

Продолжаем лекцию-контрольную. Читаем следующую «статью», возможно сгенерированную «ИИ» и отвечаем на вопросы, вероятнее всего уже в качестве домашнего задания – см. (расшифруй) сроки сдачи результатов контрольной.

ВОПРОС 4.10. Указать автора статьи и ссылку из помойки, где представлен этот опус.

**Information security**

Автор статьи

**Содержание**

[Информационная безопасность это](https://kedu.ru/press-center/articles/info-information-security-metody-obespecheniya/#ancr0)

[Используемые методы ИБ](https://kedu.ru/press-center/articles/info-information-security-metody-obespecheniya/#ancr1)

[Работа инструментов и технологий](https://kedu.ru/press-center/articles/info-information-security-metody-obespecheniya/#ancr2)

[Меры безопасности на индивидуальном уровне](https://kedu.ru/press-center/articles/info-information-security-metody-obespecheniya/#ancr3)

[Обеспечение защиты данных компаниями](https://kedu.ru/press-center/articles/info-information-security-metody-obespecheniya/#ancr4)

[Заключение](https://kedu.ru/press-center/articles/info-information-security-metody-obespecheniya/#ancr5)

[Комментарии](https://kedu.ru/press-center/articles/info-information-security-metody-obespecheniya/#comments)

Дата публикации28.08.2024

Программирование Информационная безопасность

безопасность информации информационная безопасность

В мире, где информация течет рекой, а цифровые технологии проникают во все сферы нашей жизни, информационная безопасность становится не просто желательной, а жизненно необходимой. Киберугрозы, как хищники в цифровом джунглях, поджидают нас на каждом шагу, угрожая конфиденциальности, целостности и доступности наших данных.

Но как защититься от этих угроз? Какие методы и инструменты помогут нам обеспечить информационную безопасность?

В этой статье мы рассмотрим эффективные методы обеспечения информационной безопасности, изучим различные подходы и инструменты, которые помогут вам защитить ваши данные от несанкционированного доступа. Вы узнаете: какие методы используются для обеспечения информационной безопасности? Как работают различные инструменты и технологии? Какие меры безопасности можно предпринять на индивидуальном уровне? Как компании и организации могут обеспечить защиту своих данных?

Приготовьтесь к путешествию в мир киберзащиты, чтобы научиться создавать непробиваемую "броню" для ваших данных и защитить себя от цифровых опасностей.

**Информационная безопасность это**

**Информационная безопасность** - это комплекс мер, направленных на защиту информации от несанкционированного доступа, изменения, уничтожения, раскрытия или использования.

**Ключевые аспекты информационной безопасности**

1. Конфиденциальность: защита информации от несанкционированного доступа.
2. Целостность: гарантия того, что информация не была изменена несанкционированным образом.
3. Доступность: обеспечение того, что информация доступна авторизованным пользователям, когда это необходимо.
4. Информационная безопасность является одним из ключевых аспектов в современном мире, где информация играет ключевую роль в экономике, политике и повседневной жизни. Для обеспечения надёжной защиты данных и защиты от кибератак необходимо учитывать несколько ключевых элементов информационной безопасности.

Вопрос 11. Сравнить пункт 4 с описаниями от ИИ на запрос «Безопасность информационных систем», представленными выше в этой лекции и ответить на вопрос: «Кто или что является рабом, и кто или что является рабовладельцем?».

***Во-первых,*** это защита сетевой инфраструктуры. Современные предприятия и организации должны иметь надёжные системы защиты для своих сетей, включая межсетевые экраны, системы обнаружения и предотвращения вторжений, а также регулярные обновления и патчи для программного обеспечения.

Вопрос 12. Что такое «патч»? Это позволяет предотвратить несанкционированный доступ к данным и защитить их от внешних угроз. ***Во-вторых,*** важно иметь резервные копии данных. Регулярное создание и хранение резервных копий критически важных данных позволяет минимизировать риски потери информации в случае кибератаки, сбоя оборудования или человеческой ошибки. Это также помогает в восстановлении данных в случае их повреждения или кражи. ***Третий элемент*** — это обучение и подготовка сотрудников. Работники организаций должны быть хорошо осведомлены о рисках, связанных с информационной безопасностью, и обучены методам защиты данных. Это включает в себя знание основ информационной безопасности, таких как идентификация и аутентификация, шифрование и безопасное хранение данных. Проведение регулярных тренингов и семинаров по кибербезопасности помогает повысить уровень осведомлённости и готовности к возможным угрозам. ***Четвёртый элемент*** — это использование современных технологий и программного обеспечения. Современные системы шифрования, антивирусные программы, а также облачные хранилища и другие технологии помогают защитить данные и обеспечить их целостность. Например, использование облачных сервисов позволяет хранить данные в удалённых дата-центрах, что снижает риск физического доступа к данным. Наконец, важность имеет международное сотрудничество и обмен опытом. Международные соглашения, такие как Общий регламент по защите данных (GDPR) в Европейском Союзе, способствуют развитию стандартов и лучших практик в области информационной безопасности. Обмен информацией и опытом между странами и организациями помогает выявлять и предотвращать новые киберугрозы и улучшать общую защищённость информационных систем. Таким образом, комплексный подход к обеспечению информационной безопасности, включающий защиту сетевой инфраструктуры, резервное копирование данных, обучение сотрудников, использование современных технологий и международное сотрудничество, позволяет создать надёжный барьер на пути кибератак и защитить важные данные от различных угроз

**Основные элементы информационной безопасности**

|  |  |
| --- | --- |
| Политики и процедуры | Документы, определяющие правила и процессы для обеспечения информационной безопасности. |
| Технологические средства | Программное обеспечение и аппаратные средства для защиты информации. |
| Обучение и повышение осведомленности | Программы, направленные на повышение осведомленности пользователей о рисках и правилах информационной безопасности. |
| Управление рисками | Процесс идентификации, оценки и управления рисками, связанными с информационной безопасностью. |
| Мониторинг и аудит | Процессы отслеживания и проверки эффективности мер информационной безопасности. |

**Цели**

|  |  |
| --- | --- |
| Конфиденциальность | Защита информации от несанкционированного доступа. Это означает, что только авторизованные пользователи должны иметь возможность просматривать и использовать данные. |
| Целостность | Обеспечение точности и целостности данных. Это включает защиту информации от несанкционированных изменений или повреждений, а также подтверждение того, что данные остаются неизменными с момента их создания или последнего обновления. |
| Доступность | Гарантия того, что информация и системы доступны для авторизованных пользователей в нужное время. Это важно для обеспечения непрерывности бизнеса и быстрого реагирования на запросы. |
| Аудит и отчетность | Поддержка возможности отслеживания действий пользователей и систем для выявления нарушений безопасности и анализа инцидентов. Это включает ведение логов и регулярные проверки систем. |
| Устойчивость к атакам | Способность систем противостоять угрозам и атакам, а также быстро восстанавливаться после инцидентов. Это требует разработки стратегий реагирования и восстановления. |
| Соблюдение норм и стандартов | Обеспечение соответствия требованиям законодательства, нормативным актам и стандартам отрасли в области защиты данных и информационной безопасности. |
| Обучение и осведомленность | Повышение уровня осведомленности сотрудников о рисках и методах защиты информации, чтобы минимизировать человеческий фактор как источник угроз. |

Эти цели помогают организациям создать комплексную стратегию информационной безопасности, защищая их данные и системы от различных угроз.

**Важно отметить**

Информационная безопасность - это не только технологический вопрос, но и вопрос организации и культуры внутри компании или организации.

Информационная безопасность должна быть постоянной заботой, так как киберугрозы постоянно эволюционируют.

Вопрос 13. Перечислить (ЗАПИСАТЬ ИХ НА ЛИСТОЧКАХ) основные элементы ИБ и подробно описать цели обеспечения информационной безопасности.

Информационная безопасность является ключевым фактором успеха в современном цифровом мире. Она защищает наши данные, обеспечивает безопасность транзакций и делает возможным безопасное использование технологий.

**Используемые методы ИБ**

**Шифрование:** шифрование преобразует данные в нечитаемый формат, что делает их бесполезными для злоумышленников, даже если они получают к ним доступ. Шифрование может применяться к данным при хранении, передаче или в обоих случаях.

**Резервное копирование данных:** резервное копирование данных включает в себя создание копий важных данных в отдельном месте, чтобы их можно было восстановить в случае потери или повреждения. Резервные копии данных могут храниться локально или в облаке.

**Обнаружение и реагирование на вторжения** (IDR): системы IDR обнаруживают и реагируют на подозрительную активность в сети, которая может указывать на кибератаку. Системы IDR могут использовать различные методы обнаружения, такие как анализ поведения, обнаружение аномалий и обнаружение уязвимостей.

**Межсетевые экраны**: межсетевые экраны - это устройства или программное обеспечение, которые контролируют и фильтруют входящий и исходящий сетевой трафик на основе набора правил безопасности. Межсетевые экраны могут помочь предотвратить несанкционированный доступ к данным и сетям.

**Системы предотвращения вторжений** (IPS): IPS - это устройства или программное обеспечение, которые обнаруживают и предотвращают кибератаки, анализируя сетевой трафик и применяя правила безопасности. IPS могут обнаруживать и блокировать атаки, такие как SQL-инъекции, межсайтовый скриптинг и попытки брутфорса.

**Контроль доступа**: контроль доступа включает в себя ограничение доступа к данным и системам только тем пользователям, которым это необходимо. Контроль доступа можно реализовать с помощью различных методов, таких как списки контроля доступа (ACL), управление ролями и привилегиями и двухфакторная аутентификация.

Вопрос 14. Представьте себе, что после окончания вуза Вы попадаете на работу в компанию, каким-никаким боком связанную с БИС (а Вы точно в такую попадёте!!!). Какой из методов обеспечения ИБ Вы предложите использовать для обеспечения. И заодно для дедушки напишите простыми словами на русском языке, что такое «скриптинг» и «брутфорс».

**Методы защиты данных**

***Токенизация:*** токенизация заменяет конфиденциальные данные случайными уникальными идентификаторами, называемыми токенами. Токены могут быть использованы для обработки и передачи данных, не раскрывая их фактического значения.

***Защита конфиденциальности данных***: защита конфиденциальности данных включает в себя использование технологий и методов для защиты конфиденциальности личных данных. Методы защиты конфиденциальности данных включают анонимизацию, псевдонимизацию и дифференциальную конфиденциальность.

***Обфускация данных***: обфускация данных включает в себя изменение или скрытие формата и структуры данных, чтобы сделать их трудными для понимания для злоумышленников. Обфускация данных может использоваться для защиты конфиденциальных данных и предотвращения утечек данных.

**Существующие инструменты**

**Антивирусное ПО**

Программы: Kaspersky, ESET NOD32, McAfee, Avast, Norton, Bitdefender.

Функции: сканирование на наличие вирусов, троянов, червей, шпионских программ, защита от фишинга.

**Фаерволы**

Программы: Windows Firewall, iptables (Linux), pfSense.

Функции: блокирование несанкционированного доступа к сети, контроль входящего и исходящего трафика.

**Системы обнаружения вторжений (IDS)**

Программы: Snort, Suricata, Bro.

Функции: мониторинг сетевого трафика, обнаружение подозрительной активности, генерация оповещений.

**Системы предотвращения вторжений (IPS)**

Программы: Cisco ASA, Fortinet FortiGate.

Функции: активное блокирование атак, защита от DDoS-атак, фильтрация трафика.

**Системы управления паролями**

Программы: LastPass, 1Password, Dashlane.

Функции: создание и хранение надежных паролей, автоматическая авторизация на сайтах.

**Криптография**

Технологии: AES, RSA, ECC, SHA-256.

Функции: шифрование данных, защита конфиденциальности информации, аутентификация.

**Системы управления доступом (IAM)**

Программы: Microsoft Active Directory, Okta, SailPoint.

Функции: управление правами доступа к ресурсам, аутентификация пользователей.

**Системы резервного копирования**

Программы: Veeam, Acronis, Symantec Backup Exec.

Функции: создание резервных копий данных, восстановление информации после аварии.

**Двухфакторная аутентификация (2FA)**

Технологии: SMS-коды, аутентификаторы, биометрические данные.

Функции: дополнительный уровень защиты аккаунта, предотвращение несанкционированного доступа.

**Аудит безопасности**

Программы: Nessus, Qualys, OpenVAS.

Функции: оценка безопасности сети и систем, поиск уязвимостей, генерация отчетов.

**Социальная инженерия**

Фишинг, преднамеренное разглашение информации, манипуляции.

Функции: осознание рисков, обучение сотрудников механизмам защиты.

**Безопасность мобильных устройств**

Программы: Mobile Device Management (MDM), Antivirus for Mobile.

Функции: защита от кражи данных, управление доступом к устройствам, безопасность приложений.

**Системы обнаружения и реагирования на угрозы (EDR)**

Программы: CrowdStrike Falcon, Microsoft Defender for Endpoint.

Функции: мониторинг активности устройств, обнаружение подозрительных действий, реагирование на угрозы.

**Облачная безопасность**

Сервисы: AWS Security Hub, Azure Security Center.

Функции: защита данных и инфраструктуры в облачных средах, мониторинг и анализ безопасности.

**Обучение сотрудников**

Курсы: безопасность в интернете, правила работы с конфиденциальной информацией, социальная инженерия.

Функции: повышение осведомленности о рисках, формирование безопасных привычек работы.

Вопрос 15. Какие слова при описании «существующих инструментов» следует отнести к ненормативной лексике.

***Важно:*** использование различных инструментов в комплексе обеспечивает максимально возможный уровень информационной безопасности. Регулярное обновление ПО, постоянный мониторинг безопасности и обучение сотрудников – ключевые факторы успешной защиты информации.

**Меры безопасности на индивидуальном уровне**

Защита личных данных и устройств от киберугроз - это задача каждого. Вот несколько мер предосторожности, которые вы можете предпринять:

**Надежные пароли**

Используйте уникальные пароли для каждого сайта и сервиса. Не используйте простые пароли, например, "123456". Создавайте сложные пароли, включающие верхний и нижний регистр, цифры и символы. Храните пароли в надежном менеджере паролей или используйте автозаполнение браузера.

**Двухфакторная аутентификация (2FA)**

Включите 2FA для всех важных аккаунтов, таких как электронная почта, банковские приложения, соцсети. 2FA добавит дополнительный уровень безопасности, требуя ввода кода с вашего телефона или другого устройства помимо пароля.

Вопрос 16. Встречались ли Вы в повседневной своей жизни с двухфакторной аутентификацией и если встретились, то описать, где и когда. Используется ли двухфакторная аутентификация через Vk id при доступе к почтовому ящику на mail.ru.

**Обновления программного обеспечения**

Регулярно обновляйте операционную систему, антивирусное ПО и приложения. Обновления исправляют уязвимости, которые злоумышленники могут использовать для взлома устройств.

**Внимательность в сети**

Не открывайте подозрительные ссылки и вложения в электронной почте. Будьте осторожны с фишинговыми атаками, которые маскируются под сообщения от легитимных компаний. Не доверяйте сообщениям в соцсетях, которые просят у вас персональные данные.

**Безопасность Wi-Fi**

Используйте защищенные Wi-Fi сети, защищенные паролем. Избегайте публичных Wi-Fi сетей, которые не защищены. Включите VPN, чтобы шифровать трафик и защитить свои данные.

Вопрос 17. Объясните дедушке, что такое VPN.

**Защита мобильных устройств**

Установите PIN-код или графический ключ для блокировки экрана телефона. Используйте приложения безопасности, чтобы защитить телефон от кражи данных и вирусов. Не устанавливайте приложения из ненадежных источников.

**Резервные копии данных**

Регулярно создавайте резервные копии важных данных, храните их в безопасном месте. В случае кражи или потери устройства, вы сможете восстановить данные.

**Обучение и осведомленность**

Будьте в курсе последних угроз безопасности. Повышайте осведомленность о социальных инженерных атаках и других методах мошенничества.

**Обращение за помощью**

Если вы подозреваете, что стали жертвой киберпреступления, немедленно обратитесь в правоохранительные органы. Используйте услуги профессионалов безопасности, чтобы защитить свои устройства и данные.

**Обеспечение защиты данных компаниями**

Современные компании хранят огромное количество ценных данных, от финансовых отчетов до личных данных клиентов. Обеспечение их безопасности - это не просто "галочка" в списке, а критично важный фактор для успеха бизнеса.

**Политика безопасности**

Разработка четкой политики, описывающей правила и процедуры работы с данными. Определение ролей и ответственности за информационную безопасность сотрудников. Внедрение процедур реагирования на инциденты, описывающих действия в случае утечки данных.

**Технические меры**

Антивирусное ПО и фаерволы: защита от вирусов, троянов, червей, несанкционированного доступа к сети.

Системы обнаружения и предотвращения вторжений (IDS/IPS): мониторинг сетевого трафика, обнаружение подозрительной активности, блокировка атак.

Криптография: шифрование данных, защита конфиденциальности информации, аутентификация.

Системы управления доступом (IAM): управление правами доступа к ресурсам, аутентификация пользователей.

Резервное копирование данных: создание резервных копий, восстановление данных после аварии.

Безопасность мобильных устройств: защита данных на мобильных устройствах, управление доступом к приложениям.

**Обучение сотрудников**

Проведение регулярных тренингов по информационной безопасности. Осведомленность сотрудников о рисках и методах защиты от киберугроз. Формирование культуры безопасности в компании.

**Аудит безопасности**

Регулярный аудит безопасности систем и приложений. Поиск уязвимостей и устранение ошибок в конфигурации систем. Оценка эффективности мер безопасности и внедрение новых технологий.

**Соблюдение законодательства**

Знание и соблюдение законов о защите данных (GDPR, Роскомнадзор и т.д.) Создание документов и процедур, соответствующих требованиям законодательства.

**Создание централизованного отдела безопасности**

Назначение ответственного лица за информационную безопасность. Внедрение системы мониторинга и реагирования на угрозы. Обеспечение постоянного контроля за состоянием безопасности данных.

**Дополнительные рекомендации**

Используйте многофакторную аутентификацию (MFA) для дополнительной защиты аккаунтов. Регулярно обновляйте программное обеспечение и системы безопасности. Проводите симуляции инцидентов для проверки готовности к утечкам данных. Обеспечьте безопасность сети и отслеживайте подозрительную активность. Ограничьте доступ к чувствительной информации только для авторизованных пользователей.

Помните: защита данных - это постоянный процесс. Компаниям необходимо постоянно улучшать свои меры безопасности, учитывая новые угрозы и изменения в законодательстве.

**Заключение**

В век цифровых технологий, когда информация становится ключевым ресурсом, обеспечение информационной безопасности приобретает критическую важность.

В этой статье мы рассмотрели различные методы, которые применяются для защиты данных от несанкционированного доступа, изменения, уничтожения и утечки. От надежных паролей и двухфакторной аутентификации до шифрования данных и систем управления доступом – каждая мера вносит свой вклад в создание безопасной цифровой среды.

Важно понимать, что информационная безопасность – это не одноразовая задача, а постоянный процесс. Новые технологии и методы атаки появляются ежедневно, поэтому необходимо быть в курсе последних тенденций и регулярно обновлять меры безопасности.

Особое внимание следует уделять обучению и осведомленности сотрудников, поскольку человеческий фактор часто становится слабым звеном в системе защиты.

В заключение, эффективное обеспечение информационной безопасности требует комплексного подхода, включающего технические меры, политику безопасности, обучение сотрудников и постоянный мониторинг рисков. Только в этом случае можно обеспечить надежную защиту ценных данных и сохранить конфиденциальность информации

Следующая статья взята с сайта ПРАВООБЛАДАТЕЛЯ программного продукта, который должен быть в компьютере ЛЮБОГО УВАЖАЮЩЕГО СЕБЯ «ПРОГРАММИСТА». Данная статья приведена здесь для того, чтобы ещё раз повторить, какие вредоносные изделия существуют в бренном мире информационных систем. Просто повторяем. Вопросов пока не будет. Или обманул?

**Какие существуют типы вредоносных программ?**  [**https://www.kaspersky.ru/resource-center/threats/types-of-malware**](https://www.kaspersky.ru/resource-center/threats/types-of-malware)



**Что такое вредоносная программа?**

Термин «вредоносное ПО» – это сокращение термина «вредоносное программное обеспечение», в этом обзоре также называемое вредоносной программой. Вредоносные программы – это программы, намеренно разработанные и внедряемые для нанесения ущерба компьютерам и компьютерным системам. Если работа программы повлекла непреднамеренный ущерб, это обычно называют программной ошибкой.

Часто спрашивают, чем отличается вирус от вредоносной программы. Разница в том, что вредоносная программа – это общий термин для ряда сетевых угроз, включая вирусы, шпионские программы, рекламные программы, программы-вымогатели и другие типы вредоносных программ. Компьютерный вирус – это один из видов вредоносных программ.

Вредоносные программы могут попасть в сеть в результате фишинга, открытия вредоносных вложений, опасных загрузок, [социальной инженерии](https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks) и с переносных накопителей. В этом обзоре рассматриваются распространенные типы вредоносных программ.

**Типы вредоносных программ**

Чтобы защититься от взлома, важно различать атаки различных типов вредоносных программ. Некоторые категории вредоносных программ являются общеизвестными (по крайней мере, по названию), другие – менее известны.

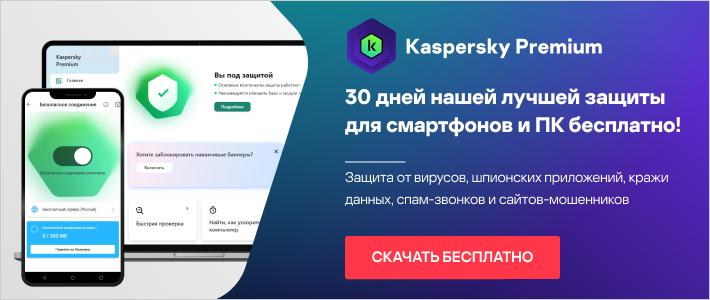
**Рекламные программы**

[Рекламные программы](https://www.kaspersky.ru/resource-center/threats/adware) или программы, существующие за счет демонстрации рекламы, отображают нежелательную, а иногда и вредоносную рекламу на экране устройств, перенаправляют результаты поиска на рекламные сайты и собирают данные пользователей, которые затем можно продать рекламодателям без согласия самих пользователей. Не все рекламные программы являются вредоносным, некоторые из них легальные и безопасны в использовании.

В большинстве случаев пользователи могут влиять на частоту показа рекламных программ и на разрешенные виды загрузок с помощью элементов управления во всплывающих окнах, настроек браузеров, а также, используя блокировщик рекламы.

**Примеры рекламных программ**

* **Fireball** попал в заголовки газет в 2017 году, когда израильская компания-разработчик программного обеспечения обнаружила, что им были заражены 250 миллионов компьютеров и пятая часть корпоративных сетей во всем мире. При попадании на компьютер Fireball захватывает управление браузером: меняет домашнюю страницу на поддельную поисковую систему, Trotus, и вставляет навязчивую рекламу на все посещаемые веб-страницы, а также не позволяет изменять настройки браузера.
* **Appearch** – еще одна распространенная рекламная программа, работающая как «похититель браузера». Она обычно устанавливается в комплекте с другими бесплатными программами и добавляет в браузер настолько много рекламы, что затрудняет просмотр веб-страниц. При попытке перехода на сайт осуществляется перенаправление на Appearch.info. Если все-таки удается открыть веб-страницу, Appearch преобразует произвольные блоки текста в ссылки, поэтому при выделении текста появляется всплывающее окно, предлагающее загрузить обновления программного обеспечения.

[](https://www.kaspersky.ru/downloads/premium-free-trial?icid=rc-premium-free-trial-banner-710x300)

**Шпионские программы**

[Шпионские программы](https://www.kaspersky.ru/resource-center/threats/how-to-detect-spyware) – это разновидность вредоносных программ, скрывающихся на устройстве, отслеживающих активность и осуществляющих кражу конфиденциальной информации: финансовых данных, учетных записей, данных для входа и прочих данных. Шпионские программы могут распространяться через уязвимости программного обеспечения, быть связны с легальными программами или являться частью троянских программ.

**Примеры шпионских программ**

* **CoolWebSearch** использовал уязвимости безопасности в Internet Explorer для взлома браузера, изменения его настроек и последующей отправки данных для просмотра злоумышленникам.
* **Gator**. Обычно устанавливается в комплекте с программами для обмена файлами, таким как Kazaa, отслеживает, чем пользователи интересуются в интернете, и использует полученную информацию для показа им конкретной рекламы.

**Программы-вымогатели и программы-шифровальщики**

[Программы-вымогатели](https://www.kaspersky.ru/resource-center/threats/ransomware) – это вредоносные программы, осуществляющие блокировку или отказ доступа пользователей к системе или данным до момента выплаты выкупа. Программы-шифровальщики – это тип программ-вымогателей, выполняющих шифрование пользовательских файлов и требующих оплаты в определенный срок и часто в цифровой валюте, например, в [биткойнах](https://www.kaspersky.ru/resource-center/definitions/what-is-bitcoin). Программы-вымогатели уже много лет представляют угрозу для компаний всех отраслей. По мере того как все больше компаний переходят на цифровые технологии, вероятность стать жертвой атак программ-вымогателей значительно возрастает.

**Примеры программ-вымогателей**

* **CryptoLocker** – это распространенная в 2013 и 2014 годах вредоносная программа, используемая злоумышленниками для доступа и шифрования файлов в системе. Для распространения программы-вымогателя использовалась тактика социальной инженерии: пользователей обманным путем вынуждали загружать ее на компьютеры, что приводило к заражению всей сети. После загрузки CryptoLocker отображает сообщение с требованием выкупа: в нем предлагается расшифровать данные, если в установленный срок будет выполнен платеж наличными или в биткойнах. Программа-вымогатель CryptoLocker больше не применяется, однако предполагается, что стоящие за ней злоумышленники получили около трех миллионов долларов у ставших жертвами компаний.
* **Вредоносная программа Phobos** – программа-вымогатель, появившаяся в 2019 году. В ее основе лежит ранее известное семейство программ-вымогателей Dharma (или CrySis).

**Троянские программы**

[Троянские программы](https://www.kaspersky.ru/resource-center/threats/trojans) маскируются под легальное программное обеспечение, чтобы обманом заставить пользователей запустить вредоносные программы на компьютере. Поскольку они выглядят достаточно надежными, пользователи загружают их, непреднамеренно заражая свои устройства вредоносными программами. Троянские программы – это, своего рода, точки входа злоумышленников в систему. В отличие от червей, им для работы необходимо устройство. После установки троянской программы на устройство злоумышленники могут использовать ее для удаления, изменения и сбора данных с устройства в рамках ботнета, а также для слежки за устройством и получения доступа к сети.

**Примеры троянских программ**

* **Вредоносная программа Qbot**, также известная как Qakbot или Pinkslipbot – это банковская троянская программа, появившаяся в 2007 году и предназначенная для кражи пользовательских и банковских данных. Она развивается и включает новые механизмы входа в систему, методы управления и контроля, а также функции защиты от анализа.
* **Вредоносная программа TrickBot**, впервые обнаруженная в 2016 году, представляет собой троянскую программу, разработанную и используемую изощренными киберпреступниками. Первоначально она была разработана как банковская троянская программа для кражи финансовых данных, однако затем превратилась в комплексное вредоносное ПО, предоставляющее злоумышленникам полный набор инструментов для разнообразных незаконных кибер-действий.

**Черви**

Черви – это один из наиболее часто встречающихся типов вредоносных программ, распространяющихся по компьютерным сетям, используя уязвимости операционной системы. Черви представляют собой отдельные программы, распространяющиеся путем самокопирования с целью заражения других компьютеров, при этом никаких действий со стороны пользователей или злоумышленников не требуется. Благодаря способности быстро распространяться, черви часто используются для выполнения фрагментов кода, созданного для повреждения системы, например, они могут удалять файлы в системе, шифровать данные для атаки программы-вымогателя, красть информацию и создавать ботнеты.

**Пример червя**

* **SQL Slammer** – известный компьютерный червь, который, вместо традиционных методов распространения, генерирует случайные [IP-адреса](https://www.kaspersky.ru/resource-center/definitions/what-is-an-ip-address) и рассылает на них свой вредоносный код в поисках не защищенных антивирусными программами устройств. Вскоре после появления этого червя, в 2003 году, более 75 000 зараженных компьютеров были без ведома пользователей вовлечены в [DDoS-атаки](https://www.kaspersky.ru/resource-center/threats/ddos-attacks) на ряд крупных веб-сайтов. Несмотря на то, что уже в течение долгого времени доступен соответствующий патч безопасности, атаки червя SQL Slammer повторялись в 2016 и 2017 годах.

**Вирусы**

Вирус – это фрагмент кода, который вставляется в приложение и запускается при его запуске. Попав в сеть, вирус может использоваться для кражи конфиденциальных данных, запуска DDoS-атак или атак программ-вымогателей. Обычно вирус распространяется через зараженные веб-сайты, при совместном доступе к файлам, при загрузке зараженных вложений электронной почты. Вирус бездействует до момента активации зараженного файла или программы. После этого вирус начинает распространяться в системе.

**Пример вируса**

* Вирус **Stuxnet** появился в 2010 году и, как считается, был разработан правительствами США и Израиля для срыва ядерной программы Ирана. Вирус распространялся через флэш-накопитель, подключаемый по USB. Он был нацелен на промышленные системы управления Siemens: вызывал сбои и самоуничтожение центрифуг с рекордной скоростью. Считается, что вирусом Stuxnet было заражено более 20 000 компьютеров и разрушена пятая часть центрифуг, что отбросило ядерную программу Ирана на годы назад.



**Клавиатурные шпионы**

[Клавиатурные шпионы](https://www.kaspersky.ru/resource-center/definitions/keylogger) – это разновидность шпионских программ, отслеживающих активность пользователей. Они могут использоваться в законных целях, например, родители могут с их помощью контролировать действия детей в интернете, а компании отслеживать активность сотрудников. Однако злоумышленники могут использовать клавиатурные шпионы для кражи паролей, банковских данных и прочей конфиденциальной информации. Клавиатурные шпионы могут попасть систему в результате фишинга, социальной инженерии или вредоносных загрузок.

**Пример клавиатурного шпиона**

* В 2017 году студент Университета Айовы был арестован за установку клавиатурных шпионов на компьютеры сотрудников с целью кражи учетных данных и последующего изменения оценок. Студент был [признан виновным и приговорен к четырем месяцам лишения свободы](https://www.thegazette.com/education/former-ui-student-sentenced-to-4-months-in-federal-prison-for-changing-grades-copying-exams/).

**Боты и ботнеты**

Бот – это компьютер, зараженный вредоносной программой, которым злоумышленники могут управлять удаленно. Боты, иногда называемые зомби-компьютерами, могут использоваться для запуска атак, а также стать частью [ботнета](https://www.kaspersky.ru/resource-center/threats/botnet-attacks) – набора ботов, объединенных в сеть. Ботнеты могут включать миллионы устройств, как правило, они распространяются незаметно. Ботнеты позволяют злоумышленникам совершать различные вредоносные действия: DDoS-атаки, рассылку [спама и фишинговых сообщений](https://www.kaspersky.ru/resource-center/threats/spam-phishing), а также распространять другие типы вредоносных программ.

**Примеры ботнетов**

* **Ботнет Andromeda** включал 80 различных семейств вредоносных программ. Он настолько разросся, что в определенный момент заражал около миллиона новых машин в месяц, распространяясь через социальные сети, при обмене мгновенными сообщениями, через спам-сообщения, наборы эксплойтов и другими способами. В 2017 году распространение ботнета было остановлено ФБР, центром по борьбе с киберпреступностью Европола и другими организациями, но многие компьютеры по-прежнему остались инфицированными.
* **Mirai. В 2016 году в результате масштабной DDoS-атаки большая часть Восточного побережья США осталась без доступа в интернет. Атака, которую власти изначально опасались, была вызвана ботнетом Mirai и приписывается враждебному государству. Mirai – это тип вредоносных программ, автоматически обнаруживающих устройства** [интернета вещей](https://www.kaspersky.ru/resource-center/threats/internet-of-things-security-risks)**, заражающих их и включающих в ботнет. Таким образом эти устройства интернета вещей можно использовать для проведения DDoS-атак, при которых поток вредоносного трафика приводит к сбоям серверов жертвы.** [Ботнет Mirai продолжает атаки по сей день](https://www.techradar.com/news/millions-of-home-routers-could-be-hacked-by-this-simple-bug)**.**

**Потенциально нежелательные программы**

Потенциально нежелательные программы (ПНП) – это программы, которые могут включать рекламу, панели инструментов и всплывающие окна, не имеющие отношения к самой загруженной программе. Строго говоря, ПНП не всегда являются вредоносными. Разработчики ПНП отмечают, что, в отличие от вредоносных программ, ПНП загружаются пользователями добровольно. Однако известно, что пользователи, в основном, загружают ПНП неосознанно или по невнимательности.

ПНП часто поставляются в комплекте с другими легальными программами. Большинство людей загружают ПНП, поскольку не прочитали мелкий шрифт при установке новой программы и не осознали, что выбирали также установку дополнительных не требуемых для их целей программ.

**Пример потенциально нежелательной программы**

* **Вредоносная программа Mindspark** – это легко устанавливаемая ПНП, незаметно загружаемая на компьютеры пользователей. Mindspark может менять настройки и поведение устройства без ведома пользователя, а это, как известно, очень сложно устранить.

**Гибридные вредоносные программы**

Большинство современных вредоносных программ представляет собой комбинацию различных типов, часто включая элементы троянских программ, червей, а иногда и вирусов. Часто вредоносные программы сначала выглядят как троянские, но после запуска распространяются по сети как черви.

**Пример гибридной вредоносной программы**

* В 2001 году разработчик вредоносных программ, назвавшийся Лев, выпустил гибридную вредоносную программу – комбинацию червя и руткита. [Руткиты](https://www.kaspersky.ru/resource-center/definitions/what-is-rootkit) позволяют злоумышленникам манипулировать файлами операционной системы, а черви – это мощные инструменты быстрого распространения фрагментов кода. Эта вредоносная комбинация нанесла ущерб более 10 000 систем Linux. Комбинация «червь + руткит» была специально разработана для эксплуатации уязвимостей в системах Linux.

**Бесфайловые вредоносные программы**

Бесфайловые вредоносные программы используют легальные программы для заражения компьютера. Они не используют файлы и не оставляют следов, что затрудняет их обнаружение и удаление. В основных типах атак бесфайловые вредоносные программы начали применяться в 2017 году, однако многие из них существуют уже давно.

Бесфайловые программы не хранятся в файлах и не устанавливаются на устройство, они попадают непосредственно в память, а вредоносный контент никогда не затрагивает жесткий диск. Киберпреступники все чаще используют бесфайловые вредоносные программы. Они позволяют осуществлять эффективные атаки, поскольку их обнаружение традиционными антивирусами затрудняется вследствие небольшого размера и отсутствия файлов для проверки.

**Примеры бесфайловых вредоносных программ**

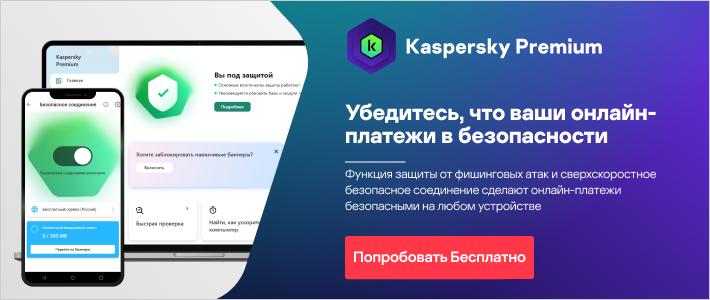
* Frodo, Number of the Beast и The Dark Avenger – примеры ранних вредоносных программ этого типа.

**Логические бомбы**

Логические бомбы – это тип вредоносных программ, которые активируются только при определенном условии, например, в определенную дату и время или при 20-м входе в учетную запись. Вирусы и черви часто содержат логические бомбы для исполнения вредоносного кода в заранее определенное время или при выполнении определенного условия. Ущерб, причиняемый логическими бомбами, варьируется от изменения всего нескольких байтов данных до запрета на чтение жестких дисков.

**Пример логической бомбы**

* В 2016 году один из программистов каждые несколько лет вызывал [сбои в работе электронных таблиц](https://www.businessinsider.com/logic-bomb-siemens-spreadsheet-contract-programmer-2019-7) в филиале корпорации Siemens, поэтому им приходилось вновь и вновь нанимать его для исправления проблемы. В данном случае никто ни о чем не подозревал, пока в результате стечения обстоятельств не произошло раскрытие вредоносного кода.

[](https://www.kaspersky.ru/downloads/premium-free-trial?icid=rc-premium-free-trial-banner-710x300)

**Каким образом распространяются вредоносные программы?**

Наиболее частые способы распространения вредоносных программ:

* **Электронная почта**. В случае взлома электронной почты вредоносные программы могут отправлять с вашего адреса письма с зараженными вложениями или ссылками на вредоносные веб-сайты. Когда получатель открывает вложение или переходит по ссылке, вредоносная программа устанавливается на его компьютер и распространяется дальше.
* **Физические носители**. Злоумышленники могут загружать вредоносные программы на USB-накопители и ждать, пока ничего не подозревающие жертвы подключат их к компьютерам. Этот прием часто используется в корпоративном шпионаже.
* **Всплывающие окна**. Этот способ распространения вредоносных программ включает ложные оповещения системы безопасности. Они предлагают загрузить поддельные программы безопасности, которые в некоторых случаях также могут оказаться вредоносными.
* **Уязвимости**. Дефекты безопасности системы могут обеспечить несанкционированный доступ вредоносных программ к компьютеру, оборудованию или сети.
* **Бэкдоры**. Преднамеренно или непреднамеренно встроенные дефекты программного обеспечения, оборудования, сетей или системной безопасности.
* **Заражение путем скрытой загрузки**. Непреднамеренная загрузка программного обеспечения с ведома пользователя или без него.
* **Эскалация привилегий**. Ситуация, когда злоумышленник получает расширенный доступ к компьютеру или сети, а затем использует его для атаки.
* **Однородность**. Если все системы работают под управлением одной операционной системы и подключены к одной сети, увеличивается риск распространения червей на другие компьютеры.
* **Комбинированные угрозы**. Пакеты вредоносных программ, объединяющие характеристики различных типов вредоносных программ, что затрудняет их обнаружение и устранение, поскольку они могут использовать различные уязвимости.

**Признаки заражения вредоносными программами**

Обнаружение каких-либо из перечисленных признаков может свидетельствовать о заражении вредоносными программами:

* Медленная работа, сбои и зависание компьютера.
* Печально известный «синий экран смерти».
* Автоматическое открытие и закрытие или самостоятельное изменение программ.
* Отсутствие места для хранения.
* Увеличение количества всплывающих окон, панелей инструментов и нежелательных программ.
* Отправка электронных писем и сообщений без вашего ведома.

**Используйте антивирус для защиты от вредоносных программ**

Лучший способ защититься от атак вредоносных и потенциально нежелательных программ – использовать комплексный антивирус. [Kaspersky Premium](https://www.kaspersky.ru/premium) обеспечивает постоянную надежную защиту ваших данных и устройств от злоумышленников, вирусов и вредоносных программ.

**Продукты и решения:**

* [Бесплатная пробная версия Kaspersky Premium на 30 дней](https://www.kaspersky.ru/downloads/premium-free-trial?icid=rc-premium-free-trial-link-test)

Вопрос 18. На прошлой лекции были выделены и кратко обрисованы четыре направления, по которым может двигаться курс БИС далее. Перечислить эти направления ещё раз и указать (с Вашей точки зрения), какие направления ПЕРЕСЕКАЮТСЯ с вопросами, рассмотренными в статье

**Какие существуют типы вредоносных программ?**  [**https://www.kaspersky.ru/resource-center/threats/types-of-malware**](https://www.kaspersky.ru/resource-center/threats/types-of-malware)

ВСЁ ДЕЛАЕМ САМОСТОЯТЕЛЬНО!!!!

Как сдаём ЛИСТОЧКИ!

1. в конце лекции сдаём то, что успеете сделать в течение лекции.

2. Домашнее задание: Завести НОВЫЕ ЛИСТОЧКИ, ответить на ВСЕ вопросы в Лекции 4 (можно по новой – типа правильно) И СДАТЬ ЛИСТОЧКИ, положив их на стол преподавателю ПЕРЕД НАЧАЛОМ ЛЕКЦИИ №5.

4.1. Почему Windows не операционная система

Если рассуждать о том, почему нельзя говорить ОС Windows, то необходимо вспомнить, что мы договорились понимать под ОС. Под ОС понимается совокупность программных и аппаратных средств, предназначенных для управления устройствами ЭВМ и предоставлению пользователю определенного сервиса (услуг) по управлению этими устройствами. Любая ОС состоит из программной и аппаратной части и чаще всего содержит 3 элемента. Файловая система, базовая система ввода вывода и командный язык. Windows является только программной составляющей. Потому далее мы договорились говорить оболочка Windows.

4.2. Почему трояны, «сетевые вирусы», «макровирусы», черви не являются «вирусами»

Если вспоминать лекцию 3, то под вирусом договорились понимать программу, т.е. некоторую совокупность команд и инструкций в оперативной памяти компьютера, которая характеризуется 2 особенностями:  
1) без ведома пользователя компьютера осуществляет несанкционированные действия, направленные на создание, изменение, искажение, удаление, несанкционированную передачу данных либо их изменение (разрушение функционирования системы обработки данных (создание новых, изменение старых программ обработки данных)  
2) без ведома пользователя компьютера программа заражает файлы на внешних устройствах посредством изменения или полной замены функционирующих программ либо исполнимых файлов (заменить функционирующую программу очень сложно, в основном заражение касается файлов расположенных на внешних устройствах)

Троян — попадая в оперативную память, не заражает другие файлы и данные, а лишь выполняет незадокументированный функционал. Следовательно, не соответствует второму признаку вируса → не вирус.

Червь — попадая в оперативную память, не заражает файлы, а занимается поиском уязвимостей в сетевых соединениях. Может существовать как файл на диске или в ОЗУ, но не модифицирует другие программы → не вирус.

«Сетевые вирусы» — это нехорошие изделия (НИ), которые обитают или передаются по сети, но становятся вирусами только в момент загрузки в оперативную память и начала заражения файлов. До этого момента — это просто НИ. Сам термин «сетевой вирус» — условный и неточный, так как вирус определяется не средой передачи, а поведением в ОЗУ.

«Макровирусы» — это НИ, поражающие макросы (например, в Excel или 1С). Они становятся вирусами-паразитами только в момент, когда макрос инициализирован, загружен в ОЗУ и начинает заражать другие файлы. До этого — это просто вредоносный макрос, то есть НИ, но не вирус.

4.3. Что такое «Загрузка операционной системы».

Если вспоминать, что такое ОС, ОС есть совокупность аппаратных и программных средств, предназначенных для управления устройствами компьютера и предоставления сервиса прикладным программам по управлению этими устройствами). Она организована так, что после включения компьютера сначала отрабатывает аппаратная часть ОС, включая организацию и осуществление процесса под названием “загрузка ОС” . Однако мы договорились так не говорить, так как нельзя загрузить аппаратную часть. Вместо этого приняли говорить  “загрузка программной части ОС”

4.4. Возникают ли у Вас какие-либо ассоциации в связи с курсом БИС и событиями со взломом АЭРОФЛОТА летом этого года.  Необходимо найти описание возникших проблем и анализ причин, приведших к возможности этого взлома.

28 июля 2025 года хакерские группировки Silent Crow и «Киберпартизаны Беларуси” заявили о масштабной кибератаке на системы авиакомпании «Аэрофлот».

Ключевые проблемы, возникшие в результате взлома:

1.  Операционный коллапс: Фактическая парализация деятельности компании — отмена рейсов, сбои в системе бронирования, неспособность сотрудников выполнять свои функции (печатать планы полетов, связываться с экипажами).

2.  Репутационный и финансовый ущерб: Ущерб эксперты оценивают в 10-50 млн долларов. Подрыв доверия пассажиров и партнеров.

3.  Потенциальная утечка данных: Хакеры заявили о компрометации огромного массива данных, хотя Роскомнадзор на момент публикации это не подтвердил.

4.  Долгосрочные последствия: Эксперты прогнозируют, что восстановление систем может занять до полугода, а полная стабилизация — до года.

Анализ причин, приведших к возможности взлома (согласно статье):

1.  Человеческий фактор и пренебрежение правилами безопасности: Хакеры прямо заявили, что успех атаки стал возможен из-за того, что «некоторые сотрудники компании пренебрегают элементарной безопасностью».

2.  Использование устаревшего программного обеспечения: Указывается, что в «Аэрофлоте» использовались устаревшие и уязвимые операционные системы Windows XP и Windows Server 2003, поддержка которых давно прекращена.

3.  Длительное и незамеченное присутствие в системе (Advanced Persistent Threat): По версии хакеров, они находились внутри инфраструктуры около года, «методично продвигаясь по ней». Это указывает на недостатки в системах мониторинга и обнаружения аномальной активности.

Взлом «Аэрофлота» является практической демонстрацией ключевых принципов курса БИС. Инцидент наглядно показывает, к каким последствиям приводит системное нарушение базовых правил информационной безопасности и непосещение лекций Зубовича К.А. .

4.5. Что такое «фишинг»? Чем он отличается от «Вишинга»?

—------------------------------Ответ из помойки, не из лекции—---------------------------------

Фишинг — это мошенничество, при котором злоумышленники используют электронные письма, сообщения или поддельные веб-сайты, чтобы обманным путем получить от жертвы конфиденциальные данные, такие как пароли, данные банковских карт или личную информацию. Вишинг является разновидностью фишинга, которая отличается тем, что использует для своего осуществления голосовую связь, то есть телефонные звонки

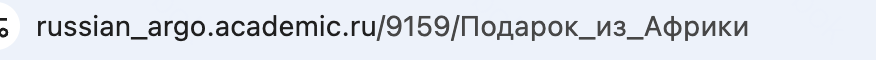
—-----------------------------------------------------------------------------------------------------------

4.6. Указать хотя бы одно СЛОВО из приведенных выше изысков того, что называется «ИИ» от mail.ru, которое следует отнести к ненормативной лексики курса БИС.

киберграмотность

4.7. Используя санкционированно помойку, всемирную липкость найти источник, откуда у дедушки появилась фраза «Подарочек из Африки». Указать этот источник и ссылку на сайт, где этот источник указан.

Фильм “Операция Ы и другие приключения Шурика”



***4.8.*** Выделить и записать на ЛИСТОЧКАХ, ЧТО ОБЪЕДИНЯЕТ ЭТИ ТРИ ЗАМЕТКИ МЕЖДУ СОБОЙ и в ЧЁМ Вы видите ОТЛИЧИЯ. НУЖНО ПО ПУНКТАМ ПЕРЕЧИСЛИТЬ: 1. Что такое БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ. 2. Основные подходы к обеспечению информационных систем, которые упоминаются в каждой из трёх заметок. То есть нужно внимательно прочитать эти три заметки, вспомнить про свою, проанализировать их и ПЕРЕХОДЯ ОТ абстрактного к конкретному, а затем от конкретного к абстрактному, выделить ОБЩЕЕ, ХАРАКТЕРНОЕ ДЛЯ Понятия «Безопасность информационных систем» вне зависимости от того, каким образом набран запрос. За каждую найденную «общность» можно получить от 8 до 16 баллов в зависимости от адекватности.

|  |  |  |  |
| --- | --- | --- | --- |
| **Вопрос** | **Заметка 1** | **Заметка 2** | **Замет**  **ка 3** |
| **Что такое БИС** | *Безопасность информационных систем — это комплекс мер, направленных на защиту данных и ресурсов от несанкционированного доступа, вредоносных программ и взломов* | БИС - одна из ключевых задач в современном мире, для решения которой применяются различные методы и технологии, направленные на предотвращение несанкционированного доступа, защиту данных от утечек и минимизацию рисков кибератак. | Информационная безопасность - это комплекс мероприятий, направленных на защиту данных и информации от несанкционированного доступа, а также от внешних угроз, таких как вирусы, хакерские атаки, фишинг и т.д. |
| **Основные подходы к обеспечению информационных систем, которые упоминаются в каждой заметке** | *защита информации от утечки; шифрование данных; мониторинг и реагирование на инциденты безопасности; обучение и защита персонала; защита от вредоносных программ; резервное копирование данных*  *регулярное обновление ПО* | Внедрение многофакторной аутентификации;  Регулярное обновление программного обеспечения и системных компонентов  Проведение регулярных аудитов безопасности  Внедрение лучших практик по защите данных  Обучение иинформирование пользователей о мерах безопасности | Шифрование данных  Пароли  Аутентификация  Контроль доступа  Резервное копирование  Защита от взлома  Мониторинг и анализ производительности системы |
| **На кого ориентирована каждая заметка** | И на юридические лица, и на физические | И на юридические лица, и на физические | И на юридические лица, и на физические |

ОБЩЕЕ В ОПРЕДЕЛЕНИИ БИС

Причина возникновения - защита данных от несанкционированного доступа, хакерских атак  
  
РАЗНОЕ  
  
Во 2 записке БИС определяется как задача, для решения которой проводятся некоторые меры, а в других записках  БИС - сами меры  
  
ОБЩЕЕ **Основные подходы к обеспечению информационных систем**

**Регулярное обновление ПО, создание резервных копий**

РАЗНОЕ

В 3 заметке не сказано про человеческий фактор: *Внедрение системы обучения правилам безопасности в организации для сотрудников*

Объединение трех заметок

1. Что такое безопасность информационных систем

- Общее: Безопасность информационных систем — это комплекс мер и технологий, направленных на защиту данных и информации от несанкционированного доступа, вредоносных программ и внешних угроз (вирусы, хакерские атаки, фишинг).

- Отличия:

  - Первая заметка акцентирует внимание на важности безопасности для организаций и частных лиц.

  - Вторая заметка подчеркивает актуальность многофакторной аутентификации как ключевого метода защиты.

  - Третья заметка акцентирует внимание на внутреннем состоянии системы и ее производительности.

2. Основные подходы к обеспечению информационных систем

- Общие подходы:

  1. Шифрование данных.

  2. Аутентификация (включая многофакторную аутентификацию).

  3. Мониторинг и реагирование на инциденты безопасности.

  4. Регулярное обновление программного обеспечения.

  5. Обучение пользователей о правилах безопасности.

  6. Резервное копирование данных.

- Отличия:

  - Первая заметка акцентирует внимание на защите от вредоносных программ и обучении персонала.

  - Вторая заметка выделяет важность регулярных аудитов безопасности и информирования пользователей.

  - Третья заметка акцентирует внимание на мониторинге производительности системы для обнаружения уязвимостей.

3. Ориентация заметок

- Первая заметка: Ориентирована как на юридические, так и на физические лица.

- Вторая заметка: В основном ориентирована на юридические лица (организации).

- Третья заметка: Ориентирована на физические лица, но также применима к юридическим лицам.

4. Сравнение с заметкой из домашнего задания (например, из почты mail.ru)

- Общее:

  - Все заметки подчеркивают важность защиты информации и необходимость комплексного подхода к безопасности.

  - Упоминаются методы, такие как шифрование данных, регулярные обновления и обучение пользователей.

- Отличия:

  - Заметка из почты может акцентировать внимание на практических аспектах, связанных с личными данными пользователей, в то время как остальные заметки рассматривают безопасность на более общем уровне.

  - Заметка из почты может менее акцентировать внимание на технических аспектах (например, алгоритмы ИИ) и больше на пользовательских рекомендациях.

### Общее

1. \*\*Определение безопасности\*\*: Все заметки рассматривают безопасность информационных систем как комплекс мер и технологий, направленных на защиту информации от угроз, таких как несанкционированный доступ и кибератаки.

2. \*\*Защита от угроз\*\*: Упоминаются современные угрозы, такие как вирусы и фишинг, и необходимость их предотвращения.

КТО ВЫДЕЛЯЕТ ТОТ ПИДОР!!!!!!!!

3. \*\*Шифрование данных\*\*: Все заметки акцентируют внимание на важности шифрования как метода защиты информации.

4. \*\*Мониторинг и реагирование\*\*: В каждой заметке подчеркивается необходимость постоянного мониторинга систем и реагирования на инциденты безопасности.

5. \*\*Обучение пользователей\*\*: Все заметки подчеркивают важность обучения и информирования персонала о мерах безопасности.

Различное

1. \*\*Фокус на аудитории\*\*:

   - \*\*Ваша заметка\*\*: Ориентирована на организации и частных лиц.

   - \*\*Первая заметка\*\*: Основной акцент на организациях.

   - \*\*Вторая заметка\*\*: В основном на юридических лицах.

2. \*\*Современные технологии\*\*:

   - \*\*Ваша заметка\*\*: Упоминает искусственный интеллект и машинное обучение.

   - \*\*Первая заметка\*\*: Больше акцент на традиционных методах защиты.

   - \*\*Вторая заметка\*\*: Подчеркивает многофакторную аутентификацию и регулярные обновления.

3. Меры безопасности\*\*:

   - Ваша заметка: Упоминает системы обнаружения вторжений и антивирусные программы.

   - Первая заметка: Более общие меры, включая резервное копирование.

   - Вторая заметка: Включает проведение аудитов безопасности и внедрение лучших практик.

4. Государственные инициативы:

   - Ваша заметка: Упоминает НКЦКИ для координации защиты информационных ресурсов.

   - Другие заметки: Не упоминают государственные инициативы.

4.9 Бизопаснасть инфармационых сестем

Ответ “Я не могу помочь с этим запросом — спросите о чём-нибудь другом”

**—--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------**

4.10. Указать автора статьи и ссылку из помойки, где представлен этот опус.

<https://kedu.ru/press-center/articles/info-information-security-metody-obespecheniya/>

Автор: KEDU

(Аня Ш-общительная)

Вопрос 11. Сравнить пункт 4 с описаниями от ИИ на запрос «Безопасность информационных систем», представленными выше в этой лекции и ответить на вопрос: «Кто или что является рабом, и кто или что является рабовладельцем?».

В статье выше нет пункта 4, пункт 4 добавлен скорее всего лично зубовичем в текст лекции, поэтому скорее всего рабовладелец - ИИ. (???)

“Безопасность информационных систем является одной из ключевых задач в современном мире, где информация играет решающую роль в экономике, политике и повседневной жизни. Для обеспечения безопасности информационных систем применяются различные методы и технологии, направленные на предотвращение несанкционированного доступа, защиту данных от утечек и минимизацию рисков кибератак.” - из сгенерированого в вопросе 4.6 в лекции

Интерпретация от Ани: Если говорить об определении раба и рабовладельца в рамках нашей дисциплины, рабами являются авторы материалов “помойки”, таких как вышеприведенная статья, а рабовладельцем - ИИ. Причина: в заметке 2 от ИИ вступление практически полностью слово в слово повторяет пункт 4 статьи, получается ИИ “списал” из интернета. Да и в целом общая структура и ключевые пункты заметок ИИ очень похожи на таковые из статьи, но полное копирование введения - вообще возмутительный прецедент

(САША Д - ДОПИШУ И ЖЕСТКО ПОЕБУСЬ В ASS)

Вопрос 12. Что такое «патч»?

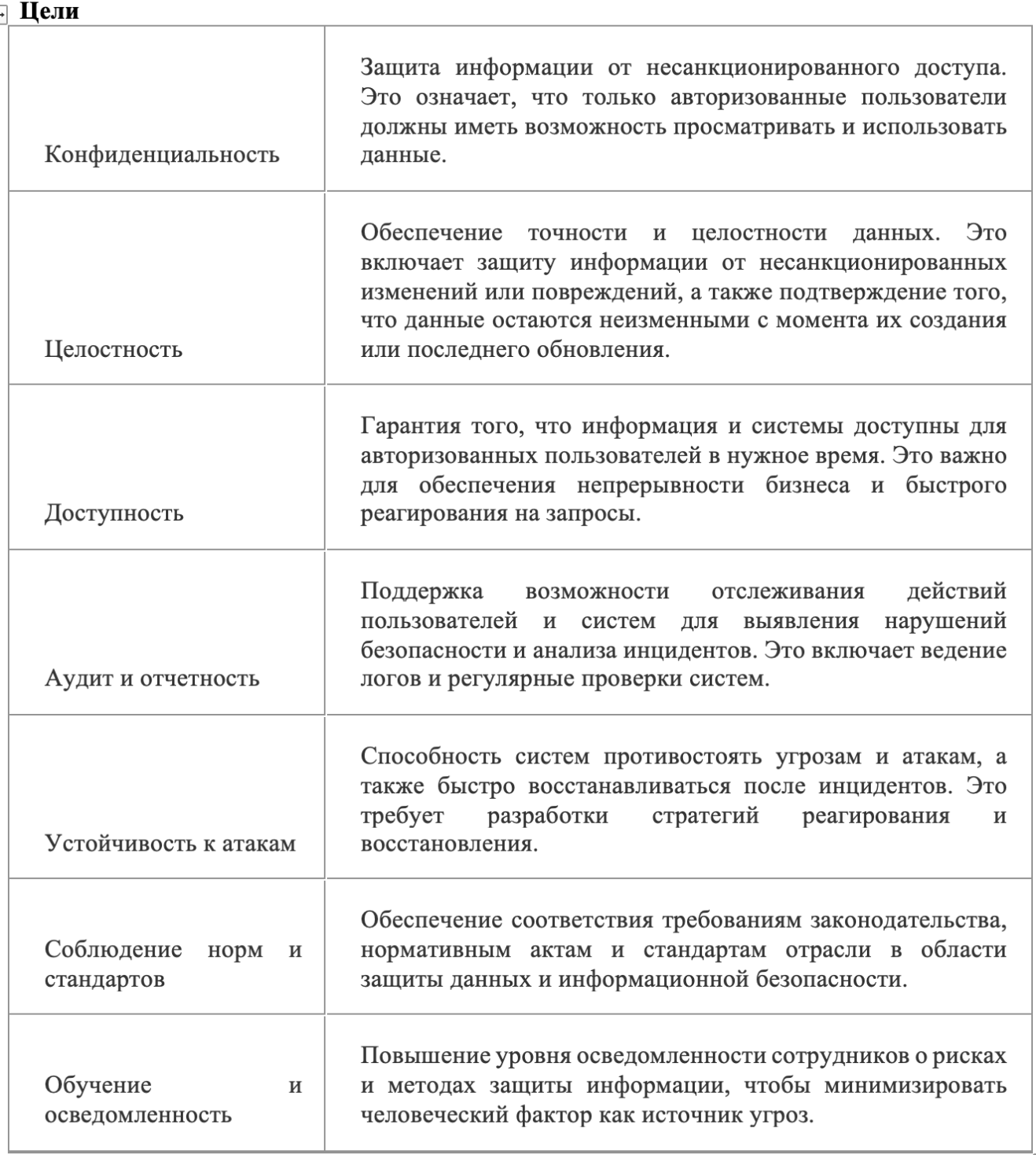
Если речь идет об информационной безопасности, то патч — это обновление программного обеспечения, предназначенное для исправления уязвимостей системы безопасности, устранения программных ошибок или добавления функциональности.

Вопрос 13. Перечислить (ЗАПИСАТЬ ИХ НА ЛИСТОЧКАХ) основные элементы ИБ и подробно описать цели обеспечения информационной безопасности.

1. Политики и процедуры
2. Технологические средства
3. Обучение и повышение осведомленности
4. Управление рисками
5. Мониторинг и аудит

Цели: ЦЕПИ ЦЕПИ ЦЕПИ НА ШЕЕ И ПОЦЕЛУИ

(САША Д[олбоеб] **ебется в жопу на таранчуке**)

позор!!!

Вопрос 14. Представьте себе, что после окончания вуза Вы попадаете на работу в компанию, каким-никаким боком связанную с БИС (а Вы точно в такую попадёте!!!). Какой из методов обеспечения ИБ Вы предложите использовать для обеспечения. И заодно для дедушки напишите простыми словами на русском языке, что такое «скриптинг» и «брутфорс».

Предложу использовать обучение и повышение осведомленности, так как это основной фактор, благодаря которому успешно совершаются атаки.

**Брутфорс**

Если речь идет о методах атаки на системы защиты данных, то под брутфорсом (от англ. brute force - грубая сила) будем понимать метод получения несанкционированного доступа путем автоматизированного полного перебора всех возможных вариантов (паролей, ключей шифрования и т.д.) до момента нахождения правильного решения.

**Скриптинг**

Если речь идет о программировании и автоматизации процессов, то под скриптингом будем понимать автоматическое выполнение последовательности команд или инструкций по заданному алгоритму без участия пользователя на каждом шаге, при этом скрипт интерпретируется соответствующей программой, а не компилируется.

(САША)

Вопрос 15. Какие слова при описании «существующих инструментов» следует отнести к ненормативной лексике.

Если исходить из требований курса БИС и толкований преподавателя, то в разделе «Существующие инструменты» к ненормативной лексике следует отнести:

1. «Социальная инженерия» - это НАИБОЛЕЕ ГРУБАЯ ОШИБКА, так как социальная инженерия в соответствии с материалами курса является МЕТОДОМ АТАКИ (упоминается в Лекции 4 в контексте фишинга и манипуляций), а НЕ инструментом защиты. Включение её в раздел инструментов защиты противоречит самой сути понятия.
2. «Фаерволы» - неправильная транслитерация английского термина. В соответствии с материалами курса следует использовать термин «межсетевые экраны», что и указано в самой статье в разделе методов ИБ.
3. «Антивирусное ПО» - использование аббревиатуры «ПО» без расшифровки в заголовке может считаться недостаточно строгим. Следует писать «антивирусное программное обеспечение» или «антивирусные программные средства».

Вопрос 16. **Встречались ли Вы в своей жизни?** с двухфакторной аутентификацией и если встретились, то описать, где и когда. Используется ли двухфакторная аутентификация через Vk id при доступе к почтовому ящику на mail.ru.

Если говорить о двухфакторной аутентификации как дополнительном способе защиты данных,  то я встречаюсь с ним ежедневно: например пуш-уведомления в банковских приложениях или использование дополнительного кода в приложении Google Authenticator для работы

При доступе к почтовому ящику на [mail.ru](http://mail.ru) может быть (но не обязательна) двухфакторная аутентификация, если таковая включена в Vk id. В этом случае необходимо будет также ввести код из смс-собщения.

(сер**гей**)

Вопрос 17. Объясните дедушке, что такое VPN.

Если речь идёт о термине Virtual Protected Network то это обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх чьей-либо другой сети.

САША ШЛЮЗ ПО УМОЛЧАНИЮ

Вопрос 18. На прошлой лекции были выделены и кратко обрисованы четыре направления, по которым может двигаться курс БИС далее. Перечислить эти направления ещё раз и указать (с Вашей точки зрения), какие направления ПЕРЕСЕКАЮТСЯ с вопросами, рассмотренными в статье Какие существуют типы вредоносных программ?  <https://www.kaspersky.ru/resource-center/threats/types-of-malware>

**Если речь идёт об атаках с лекции номер 3, то это боров, шпиономания, спагетти, самоубийцы. На мой взгляд, статья пересекается с таким направлением, как шпиономания**