Е.А. Гафарова

СБОРНИК КЕЙС-ЗАДАЧ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

Челябинск, 2023

ББК 681.14:001(021)

УДК 32.972.202я73

Г 24

Гафарова, Е.А. Сборник кейс-задач по информационной безопасности. [Текст]: Учебное пособие / Е.А. Гафарова – 122 с.

ISBN 978-5-93162-774-4

Учебное пособие включает в себя кейсы по информационной безопасности. Кейсы сгруппированы по критериям возможных вариантов их решения: от самых общих подходов и организационно-правовых мер до исследовательских и эвристических мероприятий.

Учебное пособие может быть использовано для организации практических занятий по дисциплинам «Основы информационной безопасности» и «Аппаратно-программные средства обеспечения информационной безопасности» студентов-бакалавров направления «Профессиональное обучение (по отраслям)» 44.03.04, а также для магистрантов профиля «Управление информационной безопасности в профессиональном обучении».

Рецензент: Диденко Галина Александровна, к.п.н., доцент, доцент кафедры математики, медицинской информатики, информатики и статистики, физики ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации

СОДЕРЖАНИЕ

Введение

Кейс-метод обучения — это метод активного обучения на основе реальных ситуаций. Преимуществом кейсов является возможность оптимально сочетать теорию и практику, что представляется достаточно важным при подготовке специалистов разного профиля. Отличительной особенностью этого метода является создание проблемной ситуации на основе фактов из реальной жизни.

Применение кейс-метода в образовательной практике позволяет развивать навыки работы с разнообразными источниками информации. Процесс решения проблемы, изложенной в кейсе – творческий процесс познания, подразумевающий коллективный характер познавательной деятельности. Кейс-метод используется не только как педагогический метод, но и как эффективный метод исследования, что позволяет его использовать при подготовке магистров.

Внедрение кейс-метода при обучении информатике и информационным технологиям в аспектах информационной безопасности способствует реализации компетентностного подхода.

Предлагаемый задачник позволяет комплексно формировать компетенции в области информационной безопасности, используя практико-ориентированные задачи.

Раздел 1. Общие вопросы безопасности в кейсах.

Примеры решения.

Задача 1.

Данилову пришла заработная плата. Он решает снять свои деньги через банкомат. Сняв третью часть от зарплаты, он спокойно направляется домой. Проходит некоторое время. Данилов, не тратя с карты денег, но замечает, что на балансе карты осталось меньше половины денег. Что могло спровоцировать потерю денег? Какие процедуры необходимо произвести для того, чтобы попытаться вернуть деньги обратно? Какие действия требуется выполнить, чтобы не допускать таких ошибок?

Вариант решения. Спровоцировать потерю денег могло то, что Данилов, возможно, не скрывал введение пин-кода от посторонних лиц. Пин-код мог быть записан на бумаге. И когда Данилов доставал пин-код, злоумышленник посмотрел, запомнил пин-код и запомнил какие либо данные о карте - это номер карты, дату выпуска, и трехзначный код.

Другой исход, Данилов мог, после возвращения домой, ввести на каком-либо подозрительном сайте свои банковские данные.

Для возврата своих денег оформляем претензию. Если не часто посещаете банк и проверяете состояние своего счёта, а также не пользуетесь услугами sms-уведомлений Интернет-банкинга, то обнаружить подозрительную операцию по счёту будет довольно непросто. Однако, тоже возможно. Дело в том, что банк обязан предоставлять клиенту ежемесячную выписку в конце каждого

отчётного периода, которая содержит сведения об остатке средств на счете и всех совершенных операциях. Отчётный период составляет 30-31 день и начинается, как правило, с даты выпуска карты. Банк может присылать выписку по счёту по почте (простой или электронной) на адрес, указанный в заявлении на получении пластиковой карты.

Получив очередную выписку, необходимо внимательно проверить все расчётные операции. Обнаружив операцию, которую не совершали - даже если её сумма не превышает 1000 рублей, следует обязательно обратиться в банк с претензией. Там предложат заполнить заявление установленной формы и приложить к нему все имеющиеся документы.

В случае, если операция признана мошеннической, банк в течение нескольких дней может вернуть средства клиенту, при имеющейся технологической возможности.

Способов опустошения чужих пластиковых карт великое множество, и защититься от всех практически невозможно. Однако, при соблюдении минимальных способов безопасности риски потерять деньги значительно снижаются.

Помимо основной меры безопасности, о которой предупреждают все банки, - хранить свои пластиковые карты в укромном месте и никому никогда не называть их пин-коды, а тем более писать их на видном месте, банки советуют читателям подключиться на услуги sms-банкнига, когда информация о любом движении по счёту - снятий или зачислении денег - приходит на сотовый телефон через несколько минут после совершения

транзакции. В этом случае есть возможность оперативно отреагировать на несанкционированное использование карты, позвонив в банк и заблокировав её.

Рис.1 Виртуальная безопасность - иллюстрация по запросу автора выполнена ИИ «Нейроплод».

Задача 2.

Студент Вася очень любит общаться в социальных сетях и использует свой аккаунт ВКонтакте для входа во многие сервисы сети Интернет. Вася очень доверяет своим друзьям и всегда читает их

сообщения. Они используют ВКонтакте как сервис для обмена не только сообщениями, но и фотографиями, документами, музыкой. Часто бывает такое, что Вася «вылетает» из аккаунта ВКонтакте и авторизовывается снова. «С кем не бывает» - думает он.

Однажды он заметил, что с его банковской карты произошло списание денежных средств в размере 10000 рублей.

Как это могло случиться? Какие действия должен предпринять Вася для того, чтобы вернуть свои сбережения? Что нужно сделать для профилактики возникновения подобных ситуаций?

Вариант решения. Вася использует свой аккаунт ВКонтакте для входа на другие площадки сети Интернет. Следовательно, он так же мог заходить и на сайты с платежными системами, например, АлиЭкспресс. При покупке товаров Вася мог оставить данные о своей кредитной карте: номер карты, имя владельца, CRC-код, срок действия карты, которыми и воспользовались злоумышленники. Хоть такие данные и хранятся зашифрованными, однако, не на всех сайтах, поэтому их можно получить и расшифровать, например, через cookies. А дальше развитие действий может идти по самым различным сценариям. Вася очень общительный человек, именно поэтому у него много различных друзей, но профиль любого человека можно взломать: каким образом – неважно, главное результат, и как раз-таки доверие Васи своим друзьям в плане безопасности передаваемых файлов может вызывать сомнение! Любая ссылка, документ, картинка может содержать вредоносный код, благодаря чему происходит несанкционированный выход из

социальной сети, а после повторной авторизации перехватывается пароль и логин для злоумышленника.

Видимо, у Васи также отключено оповещение ВКонтакте о том, что кто-то вошел с его аккаунта, иначе он заметил бы это. После этого возможно использование аккаунта Васи для входа на другие площадки в Интернете для того, чтобы получить данные карты или произвести покупку какого-либо товара с этой карты.

Возможен и другой поворот событий. Вася сидел дома в своей сети с помощью Wi-Fi. Вдруг соединение потерялось, произошло переподключение к WiFi. В момент переподключения данные могли перехватить злоумышленники. То же самое могло произойти и при подключении к общественной сети без авторизации через мобильный телефон, где механизм перехвата данных еще проще. С любым телефоном на платформе Android, с компьютером на любой ОС можно с помощью специальных программ заставить перезагрузиться роутер и собрать все пароли пользователей, которые вводились.

А возможен и еще один вариант. Вася очень хочет узнать, кто заходит на его страницу ВКонтакте и нашел сомнительный сайт, который якобы собирает и анализирует активность пользователей на его странице. Вася ввел там данные своего аккаунта (логин, пароль) и не добился никаких результатов. Конечно же, о том, что он ввел там пароль он и не вспомнил, ведь это был надежный сайт, как он полагал.

Само списание наличных средств вполне часто встречающийся факт: некоторые магазины могут совершать покупки без подтверждения по СМС (если не подключен Мобильный банк), у

некоторых стоит ограничение снятия денег без подтверждения, которое на руку злоумышленникам. Видимо, Вася не позаботился о своей банковской безопасности.

Необходимо осознавать, что кража денег с банковской карты – это преступление, поэтому необходимо написать заявление в полицию и в банк.

Алгоритм действия может быть такой: пишем заявление в полицию как можно подробней, строго соблюдая хронологию всех последних действий по карте, также указываем платёжные системы и сайты, где указывали данные своей карты, снимаем копию, относим в полицию. Далее идём в банк, где заполняем бланк о спорной операции (транзакции), пишем заявление в свободной форме с изложением всего случившегося, прикладываем копию заявления в полицию. Рассмотрение, как правило, длится не меньше месяца.

Не всегда получается вернуть украденные деньги. Может спасти страховка банковского счета от кражи, которая вернет сразу украденные деньги без ожидания выяснения обстоятельств. О страховании необходимо позаботиться заранее.

Рекомендации для Васи:

- Впредь быть осторожным и внимательно относиться ко всем ссылкам и документам, которые получаешь по почте или в социальных сетях. Не стоит открывать сразу же подозрительные файлы, так как может оказаться, что друга взломали;
- Необходимо пересмотреть все параметры безопасности в социальных сетях: двухэтапная авторизация с помощью ввода одноразового пароля, уведомления о входе в социальную сеть

- Необходимо пересмотреть безопасность банковских карт: нигде не сохранять данные карты, ограничить до минимума снятие наличных без смс-подтверждения, настроить Мобильный банк, не показывать никому свою карту и стараться скрывать от камер и людей CRC-код;
- Не подключаться к открытым WiFi, так как очень велик риск потери конфиденциальных данных;
- Стараться не заходить на площадки, связанные с покупкой и продажей товаров, через аккаунты в социальных сетях;
- Использовать разные пароли в разных интернет-площадках.

Задачи для самостоятельного решения.

Задача 1.1

Некий пользователь ПК читает ленту новостей ВКонтакте. В комментариях он видит сообщение о быстром заработке. Пользователя заинтересовало данное предложение, и он перешёл по этой ссылке. Там появилось окно ввода логина и пароля от ВКонтакте. По неопытности и незнанию пользователь вводит свои данные, после этого его аккаунт из соцсети «крадут» злоумышленники.

Какие были совершены ошибки? Как можно было бы избежать этой ситуации?

Задача 1.2

Сергей заметил, что его баланс начал очень быстро заканчиваться. В полном недоумении он звонит оператору и спрашивает: «В чём дело?». Оператор говорит, что все деньги уходят на СМС. Через некоторое время друзья Сергея говорят, что от него началась рассылка спам – сообщений.

Как это могло произойти и что теперь делать Сергею?

Задача 1.3

Данилову пришла заработная плата. Он решает снять свои деньги через банкомат. Сняв третью часть от зарплаты, он спокойно направляется домой. Проходит некоторое время. Данилов, не тратя с карты денег, замечает, что на балансе карты осталось меньше половины денег. Что могло спровоцировать потерю денег? Какие процедуры необходимо произвести для того, чтобы попытаться вернуть деньги обратно? Какие действия требуется выполнить, чтобы не допускать таких ошибок?

Задача 1.4

У офисного работника начались проблемы с программным обеспечением:

- Большинство программ перестают работать и вылетают с критической ошибкой;
- Сайты kaspersky.ru и drweb.ru не загружаются;
- Загрузка в безопасном режиме невозможна;
- Значительно снизилась производительность компьютера.

Он решил, что это – результат деятельности вируса. Определите, что это за вирус. Как его лечить? Как избежать заражения в дальнейшем?

Задача 1.5

Сотрудник фирмы «Заря» Иванов предусмотрительно хранит пароль от своей учетной записи не только в личной записной книге, а также записал его на стикере на рабочем столе, но кроме того, он сделал резервную копию в виде документа формата txt и сохранил его на флеш-накопителе. Вскоре обнаружилось, что папка с важными документами, которые находились у сотрудника Иванова на компьютере и которые ни в коем случае не должны были попасть в руки конкурентов, каким-то образом все-таки оказались у фирмы-конкурента.

Каковы возможные причины утечки информации? Как сотруднику Иванову можно избежать угрозы перехвата данных в дальнейшем?

Задача 1.6

Пользователь Валерий Валерьевич сидел в социальной сети Одноклассники. Друг со школы отправил ему заявку в друзья, через некоторое время он её принял. Затем в личные сообщения он прислал ему такое сообщение:

*«Привет, Валера. Представляешь, нашел наши фото с выпускного, хочешь, глянь! *ссылка*»*.

После перехода по ссылке он понял, что ссылка вредоносная и несет не тот материал, который Валерий ожидал увидеть. Вследствие перехода на компьютере пользователя стали появляться скрытые файлы и папки, доступа к которым он не имел.

Последовательно опишите действия Валерия Валерьевича по устранению возникших последствий и разработайте рекоменлации, чтобы он мог избежать такой ситуации в дальнейшем и сумел отличать достоверную ссылку от зловредной.

Задача 1.7

В деревенской школе 15 августа 2019г. получено распоряжение из Управления образования района, о том, что в связи с введением нового предмета «Астрономия», необходимо к 1 сентября 2019г приобрести учебники по данному предмету. При оформлении договора на поставку фирма-поставщик выслала счет Почтой России. Срок доставки 10-14 дней. После получения счета Финансовое управление района оплатит счет в течении 3-х дней.

Таким образом, к 1 сентября учебники в школу не поступят.

Рассмотреть вопросы по быстрейшей доставке счет на оплату, исходя из условий:

А) бухгалтер имеет ЭЦП;

Б) бухгалтер не имеет ЭЦП.

Задача 1.8

Иван Попов оставил машину с полным набором документов на парковке возле торгового центра. По возвращению он увидел, что из

машины из документов ничего не пропало, но все документы были перепутаны и сложены не так, как он их оставлял, к тому же пропала карта памяти. Что делать Ивану Попову в такой ситуации?

Задача 1.9

Выйдя на рабочее место после новогодних каникул, работники конструкторского бюро обнаружили, что один из ПК перестал работать. Осмотр компьютера и сверка с инвентаризационной описью показали, что из системного блока изъят модуль оперативной памяти и жёсткий диск.

Каким образом можно установить список лиц, которые имели доступ к ПК за прошедшие праздники? Что следует предпринять для ликвидации последствий инцидента?

Назовите ряд мер, которые помогут снизить риски возникновения подобных происшествий в будущем.

Перечислите несколько возможных последствий инцидента для предприятия.

Назовите дополнительные меры усиления безопасности, которые помогут снизить ущерб от указанных в сценариях предыдущего пункта последствий.

Задача 1.10

Поймал вирус на смартфоне, антивирус Dr.Web его обнаруживает как Android.Bodkel.25, Android.Bodkel.5. Пытаюсь удалить, но он не удаляется, пишет, что вышла какая-то ошибка. Что делает вирус? Как от него избавиться?

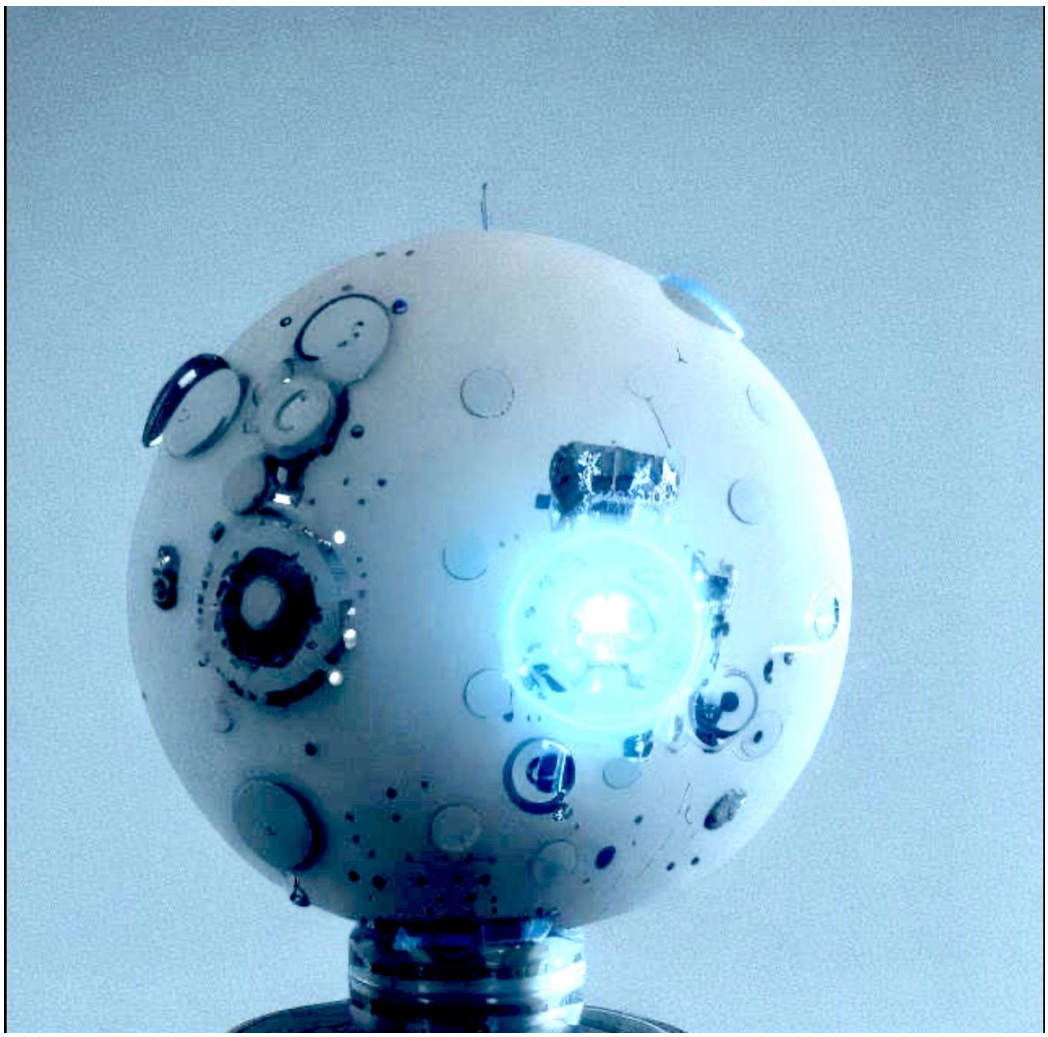


Рис. 2 – Андроид - иллюстрация по запросу автора выполнена ИИ «Нейроплод».

Задача 1.12

Я сидел со своей страницы Вконтакте. Потом вышел и зашёл с другой страницы через 2 часа и увидел, что первая страница онлайн. В чём проблема? Как её решить? Существует ли риски для нарушения информационной безопасности?

Задача 1.13

На персональном компьютере, 4 апреля в 13:00 был произведён вход на сторонний сайт развлекательного характера, требующий для

авторизации пользователя ввести код аутентификации онлайн-сервиса и платформы для потокового вещания Steam. Изначально было обнаружено, что с данного сервиса была списанная n-ная сумма средств, а также был установлен факт рассылки спама с аккаунта. При следующей попытке авторизации на данном сервисе обнаружилось, что данные, необходимые для первичной аутентификации были изменены (пароль и логин).

Что могло спровоцировать потерю данных первичной аутентификации? Какие процедуры необходимо произвести для того, чтобы попытаться восстановить данные аккаунта, а также вернуть денежные средства? Какие действия требуется выполнить, чтобы не допускать таких ошибок?

Задача 1.14

На рынке разработки медицинских препаратов против онкологических заболеваний главным ведущими конкурентами являлись две фирмы. Фирма «МедИнвест» и «Инвитро». Перед большим тендером стало известно, что в фирме «МедИнвест» произошла утечка данных, важной разработки одного из препаратов. Из-за данной утечки они проиграли тендер и деньги на разработку данных достались компании «Инвитро». В ходе расследования стало известно, что один из лаборантов, принятых на работу недавно, был бывшим сотрудником фирмы «МедИнвест». Данный сотрудник умышленно скопировал данные нового исследования и продал их на фирму конкурента «Инвитро».

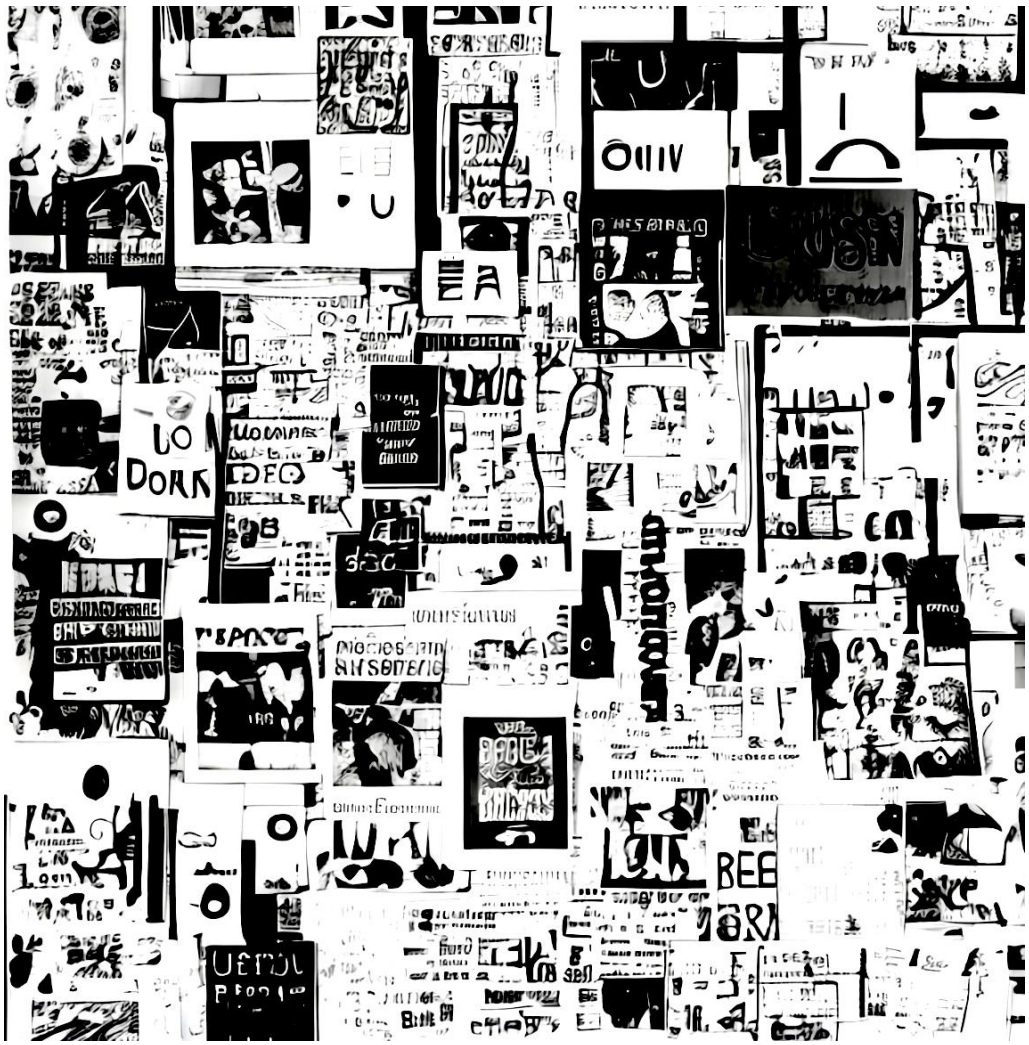


Рис.3 – Распространение информации - иллюстрация по запросу автора выполнена ИИ «Нейроплод».

Стоит отметить что:

- на сегодняшний день информационная безопасность ООО «Дайджекс Технолоджи» оставляет желать лучшего. Различная документация (техническая, экономическая) находится в открытом доступе, что позволяет практически любому сотруднику фирмы (начиная с учредителя и заканчивая водителем) беспрепятственно с ней ознакомиться;
- сотрудники не подписывают при устройстве на работу никаких соглашений о неразглашении сведений, которые относятся к

коммерческой тайне, что не запрещает им распространять подобную информацию. Набор сотрудников производится посредством собеседования, состоящего из двух этапов:

1. общение с непосредственным начальником (на котором выявляются умения и способности потенциального работника)

2. общение с учредителем (носит более личностный характер и выводом подобного диалога может быть либо «сработаемся», либо «не сработаемся»).

По каким причинам произошла утечка данных? Как в будущем фирме укрепить свои информационные базы, какие организационные меры предпринять, чтобы избежать краж данных?

Задача 1.15

В школе есть серверный диск (обменник), где хранится информация обо всех учащихся, учителя обмениваются документами, локальными актами, приказами, посредством обменника. Доступ к обменнику есть на каждом компьютере в школе, подключенном к локальной сети. Обменник никак не защищён паролем или подтверждением учетных записей. По факту, любой школьник может войти в обменник и изменить какие-либо актуальные приказы, для своей выгоды, или с целью злого умысла. Так же, в обменнике хранятся персональные данные учащихся, которые также не должны быть доступны учащимся.

Каковы могут быть последствия такой организации информационной системы? Предложите меры по минимизации уязвимостей и сокращению вероятности рисков.

Рис. 4 – Минимизация уязвимостей – иллюстрация по запросу автора выполнена ИИ «Нейроплод».

Задача 1.16

Поступил звонок из «службы безопасности банка». Обычно подобные телефонные вызовы совершают в утреннее время, чтобы застать человека врасплох. Звонки часто сопровождаются характерными фоновыми звуками большого контакт-центра. Для установления доверительного отношения звонящий обращается по имени-отчеству и даже называет примерный остаток по карте, после чего сразу же переходит к делу.

Например, сообщает, что был совершен несанкционированный вход в мобильный банк или что с вашей карты перевели денежные средства незнакомому вам лицу. Предлогов может быть огромное количество. Основная задача мошенника — сбить с толку своего собеседника.

Далее «сотрудник банка» в зависимости от ситуации пытается узнать реквизиты карты, предлагает перевести средства на резервный счет или же установить специальную программу для защиты данных, которая на деле поможет мошеннику получить доступ к сотовому телефону, а с него уже вывести средства через мобильный банк.

Как мошенники могут узнать ваш номер телефона и данные карты? Что делать, если позвонили мошенники? Есть ли какие-то сервисы проверки подозрительных номеров и сайтов?

Задача 1.17

Случай из реальной жизни! Пользователь отправил фотографии паспорта и фото себя с раскрытым паспортом на сайт для регистрации аккаунта на фрилансе. Данный сайт взломали злоумышленники, теперь требуют под давлением большую сумму денег или грозятся взять удаленный кредит на его паспортные данные и выставить их в интернет в виде, назвать пострадавшего убийцей девочки 7 лет (чтобы над ним расправились «неравнодушные люди», совершили самосуд).

Как обезопасить себя от утечки своих персональных данных? Как пострадавший должен действовать в данной ситуации? Безопасно ли отправлять свои паспортные данные в интернете?

Рис.4 – Фотограф – иллюстрация по запросу автора выполнена ИИ «Нейроплод».

Задача 1.18

В институте, на компьютере в учебной аудитории был выполнен вход в учетную запись google, в почтовый ящик gmail. Студенту необходимо было скачать лабораторную работу с почты на компьютер. После скачивания файла, студент не вышел из почты, и не очистил историю, а просто ушел от компьютера. Впоследствии было обнаружено, что изменился пароль на учетных записях от vk, steam, battle.net, Reddit и при следующих попытках зайти в эти

сервисы объявлялось сообщение что пароль не верен, как и почта. В сообщениях на почте gmail были обнаружены письма о подтверждении смены паролей и почты.

Что могло спровоцировать потерю данных первичной аутентификации? Какие действия требуется выполнить, чтобы не допускать таких ошибок? Какие процедуры необходимо произвести для того, чтобы попытаться восстановить данные аккаунтов?

Задача 1.19

Студентка Полина учится на филологическом факультете. Для выполнения одного из домашних заданий ей понадобились учебные материалы. Позаимствовав мамин ноутбук, на котором стояла Windows XP, на котором антивирус не обновлялся уже год.

Полина нашла нужные ей учебные материалы и сразу же их скачала. Файл скачался в расширении .zip. Студенка «распаковала» архив, на экране сразу же появилось окно со следующим содержанием:

«Данный ПК заблокирован по УК РФ Статья 242. Незаконные изготовление и оборот порнографических материалов или предметов. Для разблокировки ПК требуется перевести 10 000 рублей на счёт ******».

Стоит ли переводить деньги на указанный счёт? Какой тип вируса «поймала» студентка Полина? Что стоит сделать для решения проблемы? Какие меры стоит предпринять в будущем для профилактики подобных инцидентов?

Задача 1.20.

Петя захотел поиграть на компьютере в игру «Resident Evil 2 Remake», но так как Петя не хотел тратить свои деньги, он решил скачать ее бесплатно с торрента.

В браузере он ввел «скачать Resident Evil 2 Remake бесплатно торрент» и зашел на первый попавшийся сайт. Петя скачал торрент-файл, загрузил через торрент и запустил установщик. Перед установкой Петя прочитал на сайте инструкцию по установке, в которой говорилось про отключение антивируса, так как антивирус может не пропускать некоторые установочные файлы. После установки игры начали создаваться различные файлы приложений, которые невозможно удалить, выводится сервисное сообщение о том, что удалить может только администратор; компьютер начал работать медленнее; поменялись поисковик и домашняя страница в браузере, добавилось много рекламы. При запуске игры вылетает ошибка.

В чем причина изменений? Почему начали устанавливаться другие приложения? Какие действия следовало предпринять при скачивании игры? Как удалить лишние приложения и избавиться от вирусов? Какие советы можете дать Пете на будущее?

Рис.6 – Игра будущего – иллюстрация по запросу автора выполнена ИИ «Нейроплод»

Раздел 2. Организационно-правовые кейсы.

Примеры решения.

Задача 1.

Сотрудник МВД при проведении служебных совещаний, на которых обсуждались сведения, составляющие государственную тайну (далее - ССГТ), брал с собой смартфон. Им неоднократно фотографировались ССГТ, чтобы затем использовать эти сведения в служебной деятельности.

Правомерно ли был им получен доступ к ССГТ? Соблюдал ли он правила ознакомления с ССГТ? Где он мог делать пометки со служебных совещаний?

Вариант решения. Сотрудник в своей деятельности нарушил внутренний приказ министра своего ведомства а также закон о ГТ, который предписывает при обработке ССГТ использовать только учтённые носители, которые хранятся и учитываются особым образом. Его действия имели предпосылку к ознакомлению с ССГТ неограниченного круга лиц. В ходе очередного совещания, его действия были замечены начальником подразделения и было начато служебное разбирательство по данному факту. В результате этого разбирательства, при осмотре устройства и дачи показаний было выяснено, что эти фотографии пересылались сотрудником в мессенджерах коллегам по работе и было обсуждение служебных вопросов.

Действия сотрудника нарушают **ст. 12 ФЗ № 5485-1**, т.к. носитель сведений, составляющих ГТ не был учтен соответствующим

образом, на него не были нанесены реквизиты и его хранение и перемещение было бесконтрольным, что могло повлечь к разглашению сведений составляющих ГТ неограниченному кругу лиц.

Действия должностного лица подпадают под действие **ст. 283 УК РФ, ч.2** и предусматривают наказание в виде лишения свободы от 3 до 7 лет с лишением права занимать определенные должности на срок до 3 лет. Возможно, при дальнейшем разбирательстве будет установлена ответственность и по **ст. 284 УК РФ**, что предусматривает наказание в виде лишения свободы до 3 лет с лишением права занимать определенные должности на срок до 3 лет.

В деянии Шатурина можно усмотреть признаки состава преступления, предусмотренные ст. 274 УК РФ «нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей ». законодательная база для решения задачи – ст. 274 УК РФ, примечания к ст. 272 УК РФ.

Задача 2.

Студент заочного отделения Шатурин решил использовать компьютер из компьютерного класса университета для оформления контрольных и курсовых работ. Без разрешения деканата факультета он проник в класс и стал работать на компьютере. Из-за крайне поверхностных знаний и навы-ков работы на компьютере произошли сбои в работе машины, что привело в дальнейшем к отключению модема - одного из элементов компьютерной системы.

Подлежит ли привлечению к уголовной ответственности Шатурин? Дайте анализ состава преступления, предусмотренного ст.274 УК РФ.

Что понимается под информационно-телекоммуникационными сетями и оконечным оборудованием в смысле ст. 274 УК РФ? Какие виды оконечного оборудования возможны? Относится ли к оконечному оборудованию телефонный модем?

Вариант решения. Родовым объектом данного преступления являются общественная безопасность и общественный порядок; видовым – отношения в сфере компьютерной безопасности. Непосредственный объект – это отношения, обеспечивающие правила эксплуатации хранения, обработки, передачи компьютерной информации и информационно-телекоммуникационных сетей.

Объективная сторона преступления сконструирована в качестве материального состава. Обязательные условия наступления уголовной ответственности – причинение крупного ущерба. В деянии Шатурина усматриваются отдельные признаки объективной стороны деяния, в частности, нарушения правил эксплуатации информационно-телекоммуникационных сетей. Он также обладает признаками субъекта данного преступления – вменяем и достиг 16 лет. Субъективная сторона преступления характеризуется виной как в форме умысла, так и неосторожности.

Однако, вопрос об уголовной ответственности Шатурина зависит от того, в каком размере был причинен ущерб его деянием, так как состав преступления является материальным. Согласно

примечанию к **ст. 22 УК РФ** крупным ущербом в статьях данной главы признается ущерб сумма которого превышает один миллион рублей. Таким образом, Шатурин будет подлежать уголовной ответственности по **ч. 1 ст. 274 УК РФ**, если его деянием причинен ущерб на сумму свыше одного миллиона рублей.

Задачи для самостоятельного решения.

Задача 2.1

Начальник отдела новых разработок в военном НИИ ехал на доклад в вышестоящий орган управления. Для доклада им были взяты носители сведений, составляющие государственную тайну (далее – ССГТ), соответствующие грифу «Секретно». В процессе транспортировки носители были утеряны. Как были подготовлены документы к перевозке? Выделялась ли охрана, был ли проведён инструктаж перед убытием? Где и при каких обстоятельствах произошла утеря? Имел ли начальник отдела корыстный умысел?

Задача.2.2

При проведении комплексной проверки дочернего предприятия, комиссия из головного офиса отправляла сведения об основных направлениях деятельности к вышестоящим начальникам. Отправка происходила по каналам электронной почты без дополнительных мероприятий по защите информации. В результате конкурирующей фирме стали известны сведения, составляющие коммерческую тайну дочернего предприятия. Были ли выполнены мероприятия по защите коммерческой тайны? Были ли ознакомлены сотрудники предприятия

и члены комиссии с внутренними документами по обеспечению безопасности информации, составляющей КТ?

Рис.7 – Совершенно секретно – иллюстрация по запросу автора выполнена ИИ «Нейроплод».

Задача 2.3.

Сотрудник фирмы использовал в своей служебной деятельности документацию о устройстве станка, составляющую ноу-хау предприятия. Им она была получена от коллеги при переводе в отдел. При переходе из основного корпуса в технологический, по улице был

остановлен сотрудником подразделения информационной безопасности. Были ли эти сведения коммерческой тайной предприятия? Был ли ознакомлен сотрудник с перечнем сведений и с правилами работы с КТ?

Задача 2.4.

За опубликование редакцией газеты "Лабинские вести" материалов, которые содержали персональные данные несовершеннолетней гражданки, а именно фамилии, имени, сведений о школе, в которой обучается несовершеннолетняя, без ее согласия и согласия ее законного представителя, а также ряда других статей с персональными данными несовершеннолетних, Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций вынесло письменное предупреждение о недопустимости распространения через средство массовой информации сведений, составляющих специально охраняемую законом тайну, главному редактору СМИ газеты "Лабинские вести".

Однако, главный редактор не отреагировала на это предупреждение и продолжала публиковать персональные данные граждан без их согласия. Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций обратилось в Краснодарский краевой суд с исковым заявлением о прекращении деятельности газеты "Лабинские вести".

Оцените ситуацию и разрешите спор с точки зрения норм права.

Задача 2.5.

Гражданин обратился в районный суд Санкт-Петербурга с исковым заявлением к ЗАО "Издательский дом "Комсомольская правда" о признании незаконным распространение газетой "Комсомольская правда" персональных данных, а также его личного изображения.

Кроме того, гражданин просил взыскать с редакции газеты компенсацию морального вреда и опубликовать в ближайшем планируемом выпуске газеты "Комсомольская правда" опровержение. Причиной для такого обращения в суд послужил тот факт, что газета "Комсомольская правда", зарегистрированная как электронное средство массовой информации в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций опубликовала в сети интернет статью.

В этой статье содержалось интервью журналиста с гражданином с размещением его личной фотографии, а также упоминаются сведения о личной жизни гражданина, по большей части не соответствующие действительности и его персональные данные. Поскольку, гражданин уверен, что не давал такого интервью, не принимал какого-либо участия в размещении статьи, а также не давал кому-либо разрешения на опубликование своего изображения, в том числе, в данной газете, он обратился в суд. Разрешите спор согласно действующему законодательству.

Задача 2.6.

После нескольких безрезультатных попыток проверить электронную почту дома, Миша решил сходить на работу к своему отцу и повторить попытку, используя рабочий компьютер родителя. Получив одобрение отца, Миша пришел в офис во время обеденного перерыва, чтобы не отвлекать никого от работы (не нарушать течение рабочего процесса).

Когда мальчик вошел в почтовую систему, то он увидел 7 новых писем. Некоторые из этих писем он не стал просматривать, сразу определив их как спам, а остальные начал внимательно читать и отвечать на них. Особое внимание вызвало последнее письмо с заманчивой темой «Веселый прикол», полученное от Димы. После того как Миша щелкнул по пиктограмме конверта и перешел по гиперссылке, он увидел письмо и прикрепленный файл «prikol.exe».

Мальчик не стал читать письмо, так как уже заканчивался обеденный перерыв, и сразу начал скачивать прикрепленный файл. Через несколько секунд после начала скачивания, экран монитора стал черным, а системный блок начал сильно пищать.

Испугавшись, Миша позвал папу, который сразу сказал, что это опасный вирус, “гуляющий ” в настоящее время по интернету, заблокировал работу компьютера. Однако вместе с папиным компьютером были поражены до конца рабочего дня и все компьютеры, подключенные по локальной сети. Приведение компьютерной сети в рабочее состояние потребовало значительных усилий и времени. Определите, что произошло, чья вина и какова ответственность за подобного рода происшествия?

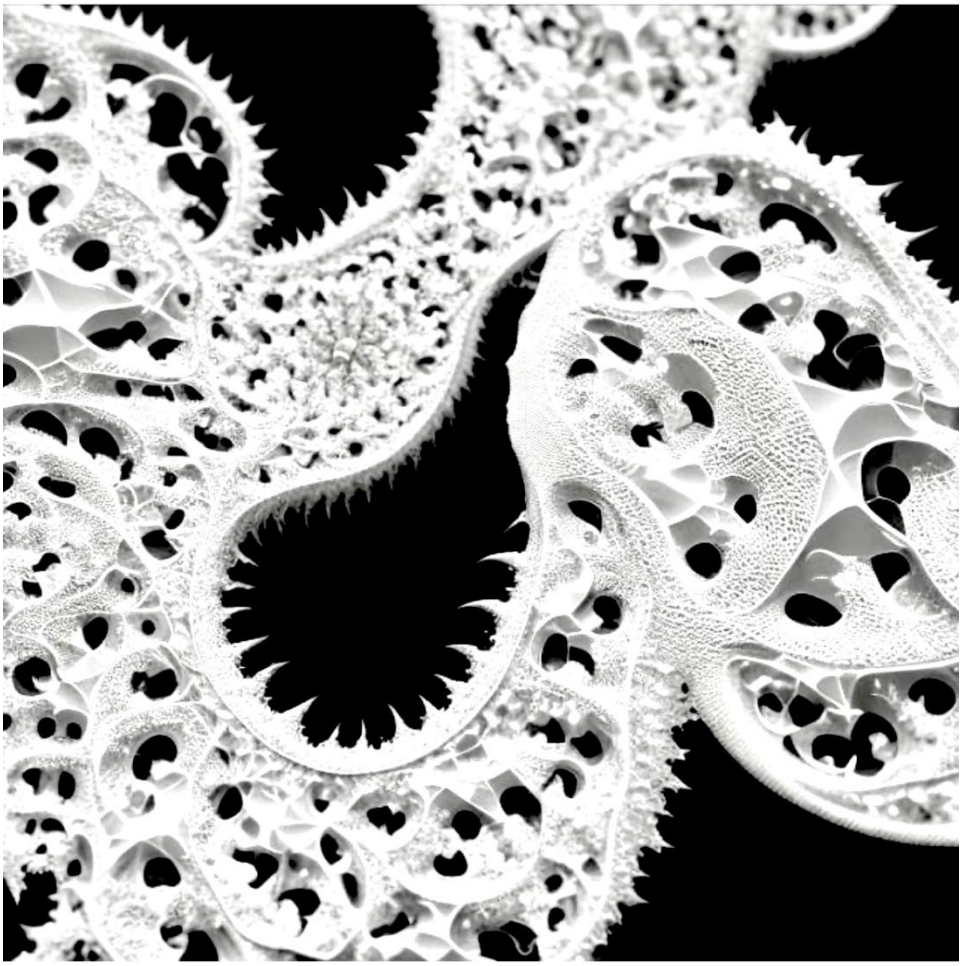


Рис. 8 – Вирусы – иллюстрация по запросу автора выполнена ИИ «Нейроплод».

Задача 2.7

Аспирант университета Хохлов занимался исследовательской работой по компьютерной "вирусологии". Целью работы было выяснение масштаба глобальной сетевой инфраструктуры. В результате ошибки в механизме размножения вирусы, так называемые "сетевые черви", проникли в университетскую компьютерную сеть и уничтожили информацию, содержащуюся в компьютерах факультетов и подразделений. В результате этого были полностью уничтожены списки сотрудников университета, расчеты

бухгалтерии по зарплате, повреждены материалы науч-но-исследовательской работы, в том числе "пропали" две кандидатские и одна докторская диссертации.

Решите вопрос о правомерности действий Хохлова. В чем заключается субъективная сторона преступлений в сфере компьютерной информации? Какова ответственность за действия Хохлова предусмотрена действующим законодательством.

Задача 2.8

Студент технического вуза Иванченко во время занятий по информатике подключился к сети "Интернет" и регулярно получал в течение семестра материалы разного содержания, в том числе и сексуального характера. В конце семестра в институт поступил запрос о работе в "Интернет" и пришел чек на оплату 105 часов пребывания в сети "Интернет". Руководство института поставило вопрос о привлечении Иванченко к уголовной и гражданской ответственности.

Дайте правовую оценку действиям студента Иванченко.

Задача 2.9

Оператор ЭВМ одного из государственных учреждений Утевский, используя многочисленные дискеты с информацией, получаемые от сотрудников других организаций, не всегда проверял их на наличие "вирусов", доверяясь заверениям поставщиков о том, что "вирусов" нет. В результате этого в компьютер Утевского, а затем и в компьютерную сеть учреждения попал комбинированный вирус,

что привело к утрате информации, содержащей государственную тайну, и поставило под угрозу срыва запуск одного из космических объектов.

Дайте юридический анализ действий Утевского. Что следует понимать под тяжкими последствиями нарушений правил эксплуатации информационно-телекоммуникационных сетей?

Рис.9 – Инцидент – иллюстрация по запросу автора выполнена ИИ «Нейроплод».

Задача 2.10

Савченко осуществлял рассылку подложных электронных писем с целью завладения персональной информацией клиентов «Ситибанка». Рассылка представляла собой электронное письмо с сообщением о переводе 100 долларов США на личный счет клиента и содержала просьбу зайти в систему Интернет-бакинта «CitibankOnline» для подтверждения перевода. В случае следования по указанной ссылке происходило попадание на сайт, созданный Савченко, и очень похожий на стартовый экран «CitibankOnline». Десять человек ввели номер кредитной карты и пин-код для того, чтобы войти в систему. Воспользовавшись полученной таким образом информацией, Савченко совершил завладение денежными средствами Павлова и Костенко, находящимися в Ситибанке, в сумме 15 и 20 тысяч долларов соответственно.

Квалифицируйте содеянное Савченко, дайте правовую оценку.

Задача 2.11

Гуляшов, студент факультета вычислительной математики, организовывал сетевые атаки, заключающиеся в получении обманным путем доступа в сеть посредством имитации соединения. Таким образом, он получил доступ к информации о счетах пользователей интернета и номерах некоторых кредитных карт и пин-кодов. Полученную информацию Гуляшов передавал Сорокиной за вознаграждение, которая использовала ее для хищения денежных средств.

Что такое фишинг, спуфинг и фарминг? Признаки какого явления усматриваются в деянии Гуляшова? Фишинга, спуфинга или фарминга? Квалифицируйте содеянное Гуляшовым и Сорокиной.

Рис.11 – Сайты – мошенники – иллюстрация по запросу автора выполнена ИИ «Нейроплод».

Задача 2.12

ГУВД Московской области было возбуждено уголовное дело по факту совершение неправомерного доступа в охраняемой законом компьютерной информации в кассовых аппаратах одного из индивидуальных предпринимателей г.Павловский-Посад Лебедева. Следствие квалифицировало действие Лебедева по ч.2 ст.272 УК РФ,

т.е. изменение информации в контрольно-кассовых аппаратах, при которых записанная в них сумма выручки за смену искусственно занижалась. Информация, содержащаяся в контрольно-кассовых аппаратах, признана следствием разновидностью компьютерной информации. Адвокат Лебедева настаивал на изменении квалификации.

Дайте юридическую оценку содеянного. Что следует понимать под компьютерной информацией?

Задача 2.13

Петров использовал доработанный сотовый телефон – «сканер», который позволял производить звонки за чужой счет. Всего в течение шести месяцев Петров таким образом «израсходовал» 15 тыс.рублей. Можно ли считать информацию, содержащуюся в сотовым телефоне, компьютерной информацией? Как соотносятся компьютерная информация и коммерческая тайна? Квалифицируйте содеянное Петровым.

Задача 2.14

Панченко и Будин, работали в компьютерной форме, распространяли «Троянские» программы и получали доступ к паролям пользователей компьютеров. Дайте анализ объективных и субъективных признаков данных составов преступлений.

Решите вопрос о квалификации содеянного и укажите нормы права, согласно которым Панченко и Будим могут быть привлечены к ответственности.

Задача 2.15

Харламова А.Е. работала в 2012 г. секретарем нотариуса в нотариальной конторе. Некто Толкачёв Л.Э. пришёл к нотариусу и оформил завещание на своего сына.

В 2018 г. Харламова А.Е. опубликовала информацию о данном завещании на своём форуме, где дочь Толкачёва Л.Э. прочитала её.

После семейного скандала Толкачёв Л.Э. обратился к Харламовой А.Е. с претензиями и просьбой удалить данные материалы с сайта, на что она ответила: *«Во-первых, я не нотариус, чтобы хранить ваши тайны. А во-вторых, я могу публиковать любую информацию на своем сайте»*

Можно ли привлечь Харламову А.Е. к ответственности? Какие нормы права нарушила Харламова А.Е.?

Задача 2.16.

Сотрудником подразделения объектового режима при выходе из лабораторного корпуса НИИ у сотрудника был обнаружен машинный носитель информации, что является нарушением регламента информационной безопасности, введённом на предприятии.

Что должен предпринять сотрудник службы безопасности, чтобы удостовериться в обеспечении информационной безопасности вверенного ему подразделения?

Раздел 3. Применение программно-аппаратных средств.

Примеры решения.

Задача 1.

На предприятии возникла необходимость отправить документы в Министерство Обороны РФ (далее МО), подписанные электронной подписью одного из руководителей. МО прислали инструкцию, ЭЦП для подписания есть у директора и его заместителя (Рутокен ЭЦП 2.0). При подписании документов ЭЦП директора, КриптоАРМ выдал ошибку: «Нет полного доверия к сертификату подписи», а после подписания документов другой подписью, при загрузке их на ресурс МО, появляется ошибка, что сертификат недействителен. При этом заведомо известно, что обе подписи действительны. Получатель посоветовал подписать документы на другом компьютере, но при установке носителя КриптоАРМ не видит сертификатов на носителях, при этом всплывает окно «Установка заблокирована групповой политикой».

Почему может появиться такая ошибка о доверии к сертификату? Можно ли проверить действительность сертификатов и как, с помощью какой программы, можно это сделать. Как решить проблему с определением сертификатов на другом компьютере?

Вариант решения. Для решения первой проблемы, необходимо загрузить список отозванных сертификатов и импортировать его в Крипто АРМ. Далее, проверить любые свойства сертификата (срок действия, информация о выданной организации и т.п.) можно с

помощью панели управления Рутокен, открыть сертификат и перейти во вкладку «Свойства»

При установке носителя в новый компьютер необходимы драйвера (в данном случае Рутокен), скорее всего на данном компьютере они отсутствуют. Сообщение «Установка заблокирована групповой политикой» может говорить о том, что USB порты отключены групповыми политиками предприятия, поэтому необходимо обратиться к системному администратору, чтобы он внес изменения в групповую политику.

Рис. 12 – Рутокен – иллюстрация по запросу автора выполнена ИИ «Нейроплод».

Задача 2. Андрей решил закупить себе скины (уникальная покраска оружия) для игры Counter-Strike: Global Offensive на сайте, где они продаются по меньшей цене, чем на торговой площадке Steam.

Час он пытался зайти на этот сайт, авторизовываясь с помощью данных аккаунта Steam. Когда ему надоело, он решил всё же купить скины на торговой площадке Steam и понял, что не может зайти в свой аккаунт. Посмотрев информацию об аккаунте через браузер, он осознал, что тот сайт был фишинговым и его данные аккаунта украли.

Как можно было обезопасить свой Steam аккаунт, чтобы его не могли взломать? Что делать теперь, после того, как данные профиля украдены?

Вариант решения. Порядок действия может быть таким:

1. Установить антивирусную программу.
2. Использовать максимально надёжный и защищённый почтовый сервис.
3. Активировать Steam Guard.
4. Придумать оригинальный и сложный пароль.
5. Никому и никогда не разглашать свой логин и пароль.
6. Сделать привязку аккаунта к номеру мобильного телефона.
7. Настроить приватность профиля под себя.
8. Быть спокойным по поводу защиты своего аккаунта.

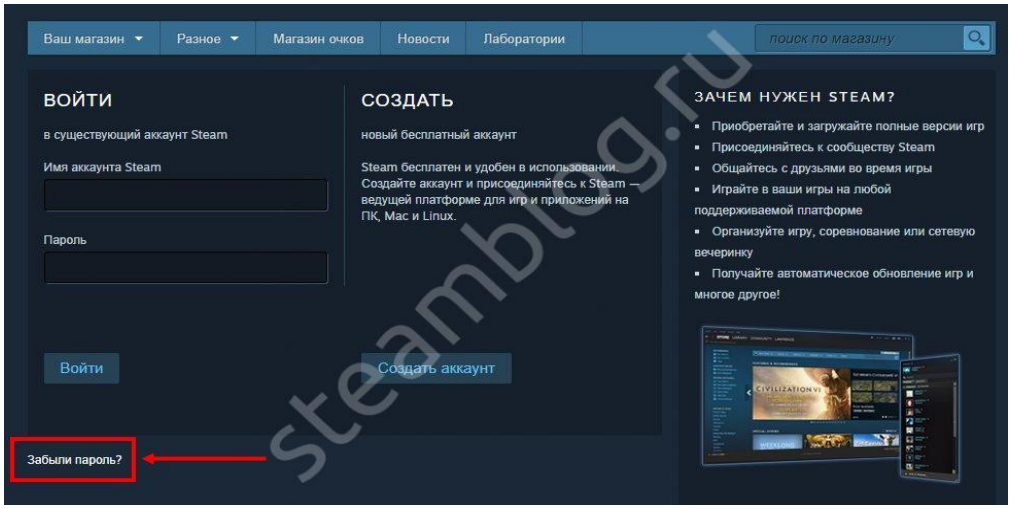
Первое, что рекомендует сделать администрация Steam при краже данных профиля — проверить компьютер на факт

вредоносных программ, которые могли украсть личные данные для входа. Если злоумышленники украли аккаунт Steam, необходимо избавиться от такого ПО, а уже после предпринимать дополнительные шаги. Для проверки используйте антивирусные программы или специальные сканеры шпионского программного обеспечения.

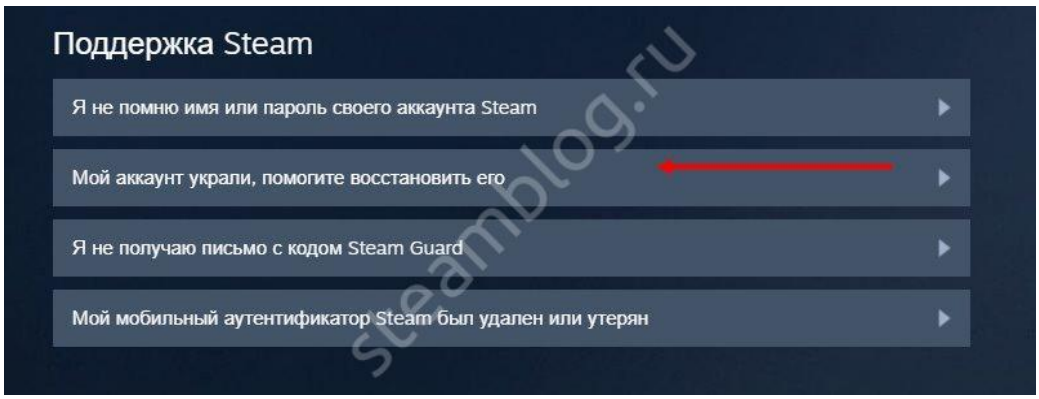
При рассмотрении вопроса, как восстановить украденный аккаунт Steam, эксперты советуют обновить пароль электронной почты. Таким способом снижается вероятность повторной кражи данных и получения доступа к учетной записи.

После выполнения рассмотренных выше действий, а именно защиты ПК и электронной почты, можно восстановить Steam-аккаунт посредством замены пароля. Для этого сделайте следующие шаги:

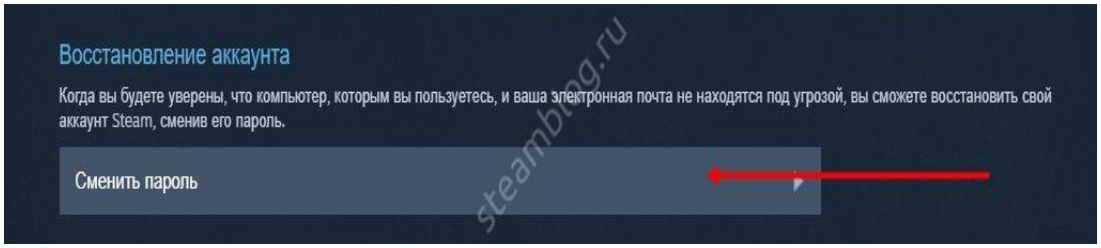
- начните выполнять вход и внизу экрана кликните на **Забыли пароль;**



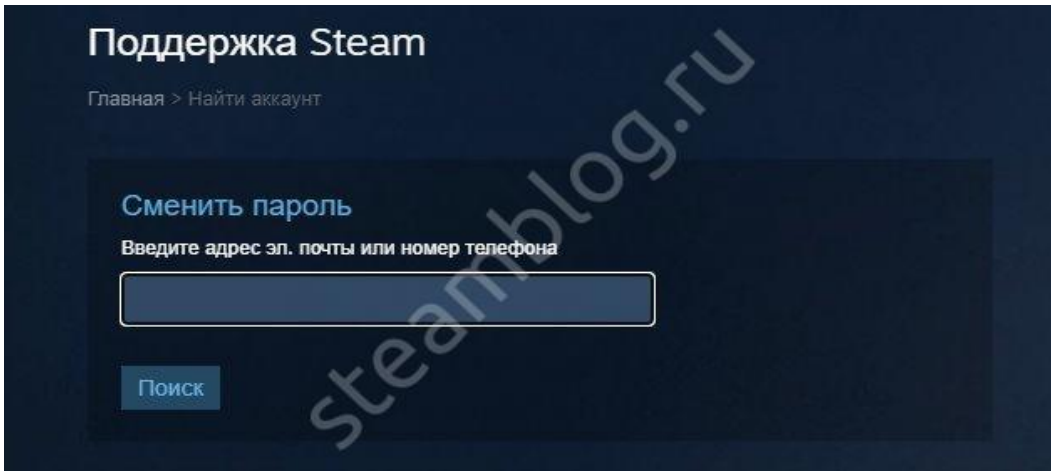
- выберете раздел **Мой аккаунт украли…**;



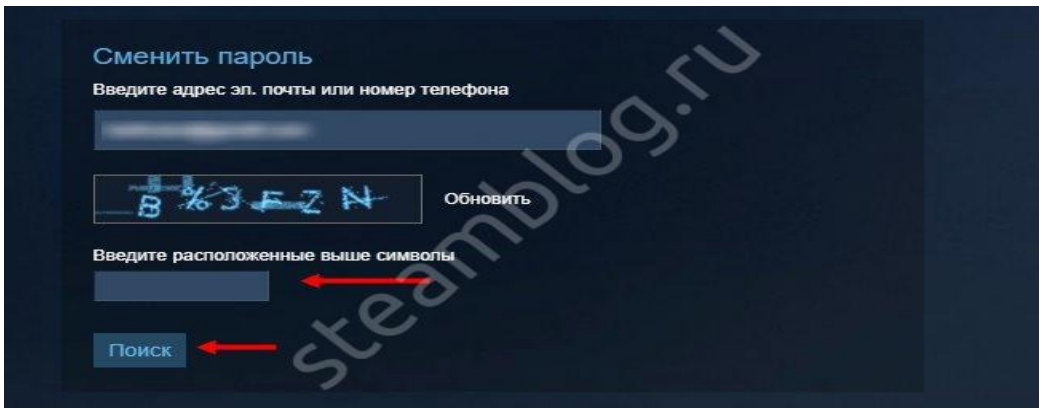
- кликните **Сменить пароль**;



- введите адрес электронной почты или телефонный номер;



- укажите капчу;
- жмите Поиск;



- выберите один из предложенных вариантов (как правило, первый);
- дождитесь получения кода на почтовый ящик;
- введите его в специальное поле;
- измените пароль и подтвердите ввод;
- запишите данные в надежном месте.

Сложней обстоит ситуация, если украли аккаунт и уже поменяли почту и пароль. Единственный выход в таком случае — написать в службу поддержки.

Задачи для самостоятельного решения.

Задача 3.1

Однажды пользователь вставил свой USB - накопитель в рабочий ПК, отправил на него необходимые файлы с это ПК. Вставив дома накопитель, им было обнаружено, что все файлы, которые были отправлены на накопитель, и, конечно же, которые были на нем, стали ярлыками.

Определить по какой причине файлы стали ярлыками. Что необходимо предпринять, чтобы восстановить все файлы? Что необходимо делать, чтобы такого больше не происходило?

Задача 3.2

Некий пользователь работал на своём ПК. Днем позже этот же пользователь запустил ПК и на экране монитора высветился синий экран с непонятными иероглифами. Определить по какой причине ПК не запускается? Что необходимо предпринять, чтобы

восстановить ОС? Что необходимо делать, чтобы такого больше не происходило?

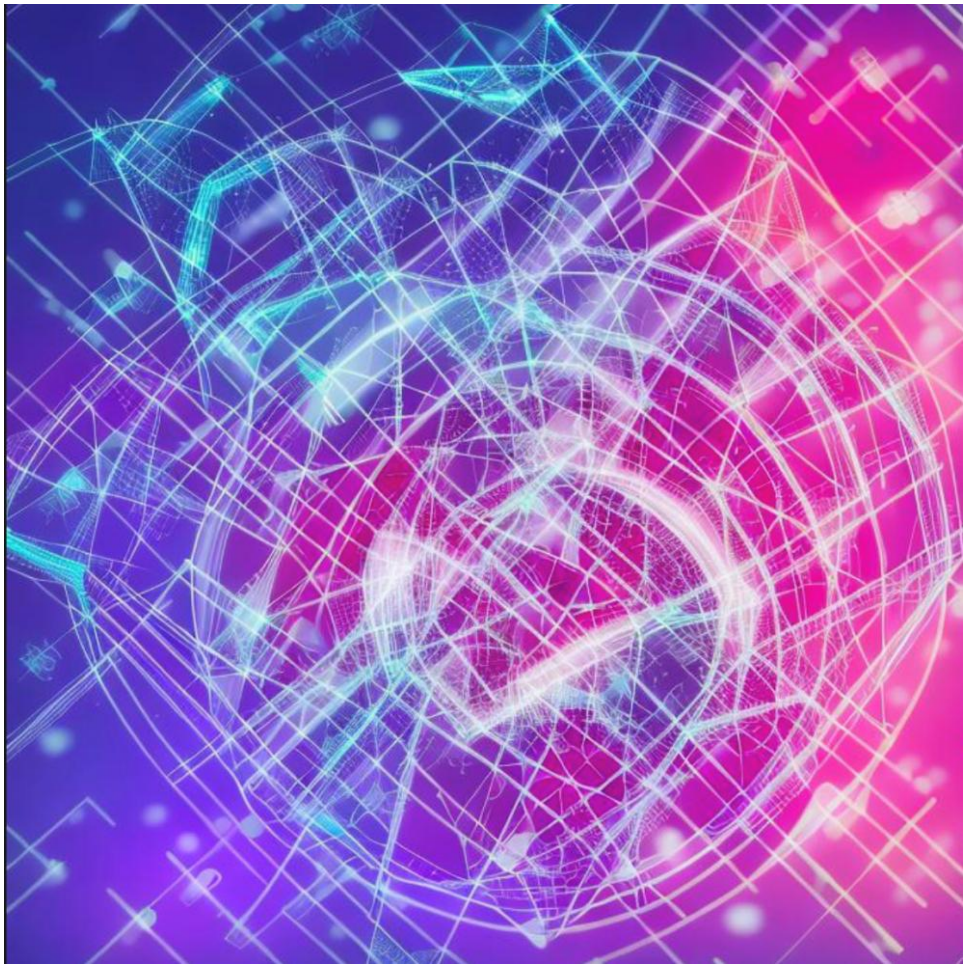


Рис. 13 – Операционная система – иллюстрация по запросу автора выполнена ИИ «Нейроплод».

Задача 3.3

В организации имеется два основных центра обработки данных и несколько филиалов. Современные тенденции ведения бизнеса предполагают наличие не только стационарных пользователей, но и мобильных. Многие сотрудники компании применяют в своей работе не только обычные рабочие места, но и мобильные устройства. Предполагается необходимость взаимодействия с партнерами и

заказчиками, с предоставлением им доступа к некоторым ресурсам компании. Внедрение корпоративной PKI обусловлено ростом потребности в обеспечении безопасности внутри предприятия. Имеется потребность в использовании и публичных удостоверяющих центров, отсутствует возможности работы внешних клиентов компании, имеется необходимость в обеспечении безопасности внутри предприятия. Как внедрить PKI для организации? Как настроить свой центр обработки данных и установить доступ клиентов компании к данным?

Теоретические сведения:

Инфраструктура открытых ключей (ИОК, англ. PKI — Public Key Infrastructure) — это термин, подразумевающий набор мер и политик, позволяющих развертывать и управлять одной из наиболее распространенных форм онлайн-шифрования — шифрованием с открытым ключом. Помимо того, что PKI является хранителем ключей для вашего браузера, он также обеспечивает защиту различных инфраструктур, включая внутреннюю коммуникацию внутри организаций, Интернета вещей (IoT), одноранговых соединений (P2P) и так далее. Существует два основных типа PKI:

• Веб-PKI, также известный как «Internet PKI», был определен RFC 5280 и дополнен CA/Browser Forum. По умолчанию он работает с браузерами и со всем остальным, что использует TLS (вы, вероятно, используете его каждый день).

• Внутренний (или локальный) PKI — это PKI, который вы используете для собственных нужд, а именно для зашифрованных локальных сетей, контейнеров данных, корпоративных ИТ-

приложений или корпоративных конечных точек, таких как ноутбуки и телефоны. В общем-то, его можно использовать для всего, что необходимо идентифицировать.

Внутри PKI имеется открытый криптографический ключ, который используется не для шифрования данных, а, скорее, для аутентификации общающихся сторон.

Рис. 10 – Криптография – иллюстрация по запросу автора выполнена ИИ «Нейроплод».

Задача 3.4

В ноябре 1988 г. случилась первая эпидемия, вызванная сетевым червем. На офисных компьютерах стояла операционная система Unix. Доступ в интернет имел один компьютер, остальные были связаны с ним по локальной сети. Это позволяло маскироваться под задачу

легальных пользователей системы. Однако из-за ошибок в коде безвредная по замыслу программа неограниченно рассылала свои копии по другим компьютерам сети, запускала их на выполнение и таким образом забирала под себя все сетевые ресурсы. Червь Морриса заразил по разным оценкам от 6000 до 9000 компьютеров в США (включая Исследовательский центр NASA) и практически парализовал их работу сроком до пяти суток.

Общие убытки были оценены в минимум 8 миллионов часов потери доступа и свыше миллиона часов прямых потерь на возобновление работоспособности систем. Общая стоимость этих расходов оценивается в 96 миллионов долларов.

Предложите варианты выявления заражения, проверки, профилактики, защиты данных.

Задача 3.5.

Новая амбициозная компания из Москвы решила создать свой собственный сервис электронной почты. На этапе разработки системы авторизации пользователей, у одного из сотрудников появилось опасение, что через их сервис, на текущий момент, злоумышленники смогут посылать письма от лица простых пользователей в своих целях. По его мнению, это возможно в случае, если пользователь войдет в систему, выполнит свои задачи, и «выйдет из системы» путем простого закрытия вкладки, то есть, фактически не выходя из системы, так как при простом закрытии вкладки пользователь остается авторизованным в системе. Также

известно, что со стороны сервера их сервис защищен в достаточной мере.

Известно, что сервер сервиса достаточно защищен от атак злоумышленников, уязвимой остается сторона клиента. Одним из самых распространенных способов атак со стороны клиента – является подделка межсайтовых запросов. Необходимо определить основные способы защиты от данного вида атак и предложить их к внедрению в проект, что позволит предупредить успешность дальнейших атак по методу подделки межсайтовых запросов.

Задача 3.6

Не работает доступ на сайт bus.gov.ru . За неделю до этого случая доступ к сайту был возможен. При попытке авторизации на сайте выдается сообщение:

А) Истек срок действия сертификата

Б) Неправильно введен пароль (нет такой ЭЦП).

Как наладить работу с сайтом bus.gov.ru?

Задача 3.7.

Утерян ключевой носитель информации, в результате чего отсутствует доступ к федеральным порталам. Опишите подробную последовательность действий для этого случая.

Задача 3.8.

На персональном компьютере был произведён вход на сторонний сайт развлекательного характера, требующий для

авторизации пользователя ввести код аутентификации онлайн-сервиса и платформы для потокового вещания Steam.

Изначально было обнаружено, что с данного сервиса была списана n-ная сумма средств, а также был установлен факт рассылки спама с аккаунта. При следующей попытке авторизации на данном сервисе обнаружилось, что данные, необходимые для первичной аутентификации были изменены (пароль и логин).

Что могло спровоцировать потерю данных первичной аутентификации и каким образом это произошло? Какие процедуры необходимо произвести для того, чтобы попытаться восстановить данные аккаунта, а также восстановить потраченные средства? Какие действия требуется выполнить, чтобы не допускать таких ошибок?

Задача 3.9.

На предприятия ООО появилась необходимость автоматизации подписания документов. Основной документ перед подписанием нужно обязательно просмотреть, чтобы убедиться в его правильности, но сервисные документы существуют для технических целей, поэтому их подписание можно автоматизировать. Предложите варианты внедрения автоматизации сервисных документов.

Задача 3.10.

У завуча школы возникла необходимость выложить электронные аттестаты на портал ФИС ФРДО, подписанные электронной подписью директора школы и зашифрованные.

При подписании электронных документов ЭЦП директора, Vip NET CSP выдал ошибку: «Нет полного доверия к сертификату подписи», но подписал файл аттестата, при загрузке его на ФИС ФРДО, появляется ошибка, что сертификат не действителен. Не известно действительна ли ЭЦП.

Почему может появиться ошибка о доверии к сертификату? Какие меры необходимо предпринять для отправки сведений об аттестатах?

Задача 3.11.

При передаче информационных ресурсов студентам для обучения, они, в целях быстрой сдачи контрольных заданий, «вскрывают код» и нарушают работоспособность программы. Какими способами можно предотвратить эти взломы?

Задача 3.12.

В отдел информационной безопасности поступил звонок из конструкторского отдела, сообщили, что файлы у сотрудника стали неизвестного расширения, а также то, что на переднем фоне окно с требованием перечислить деньги на банковскую карту.

Опишите подробный алгоритм действий.

Раздел 4. Исследовательские и эвристические кейсы.

Задача 4.1.

«Эпидемия сетевого червя»

В ноябре 1988 г. случилась первая эпидемия, вызванная сетевым червем. На офисных компьютерах стояла операционная система Unix. Доступ в интернет имел один компьютер, остальные были связаны с ним по локальной сети. Это позволяло маскироваться под задачу легальных пользователей системы.

Однако из-за ошибок в коде безвредная по замыслу программа неограниченно рассылала свои копии по другим компьютерам сети, запускала их на выполнение и таким образом забирала под себя все сетевые ресурсы.

Червь Морриса заразил по разным оценкам от 6000 до 9000 компьютеров в США (включая Исследовательский центр NASA) и практически парализовал их работу сроком до пяти суток.

Общие убытки были оценены в минимум 8 миллионов часов потери доступа и свыше миллиона часов прямых потерь на возобновление работоспособности систем. Общая стоимость этих расходов оценивается в 96 миллионов долларов.

Выступить в роли работников исследовательского центра и предложить варианты выявления заражения, проверки, профилактики, защиты. Не ограничивайтесь только программными мерами, предложите комплекс мероприятий для ликвидации последствий и долговременной программе профилактики подобных инцидентов.

Задача 4.2.

«Потеря смартфона до презентации»

В 2010 году прототип смартфона iPhone 4 был оставлен в баре одним из сотрудников компании Apple Греем Пауэллом. До официальной презентации гаджета оставалось еще несколько месяцев, но нашедший смартфон студент продал его за 5000 долларов журналистам Gizmodo, сделавшим эксклюзивный обзор новинки. Проблема состоит в том, что официальная презентация гаджета может сорваться до назначенной даты, так как до презентации все технические данные могут быть раскрыты журналистам, все функции нового смартфона и компании Apple понесет репутационный ущерб. Кроме того, на смартфоне находится информация сотрудника компании.

Как минимизировать или вовсе исключить риски при возникшей ситуации?

Задача 4.3.

«Аудит конфиденциальной информации»

Провести аудит информационных процессов фирмы, выявить критически важную информацию, которую необходимо защищать. Защита информации заключается не только в обеспечении конфиденциальности информации, необходимо обеспечить защиту информации от подделки, модификации, парирования угроз нарушения работоспособности системы. Аудит информационных процессов должен заканчиваться определением перечня конфиденциальной информации предприятия, участков, где эта

информация обрабатывается, допущенных к ней лиц, а также последствий утраты (искажения) этой информации. Таким образом, необходимо определить: что защищать, где защищать и от кого защищать. Выполните данный кейс на примере конкретного предприятия или организации.

Задача 4.4.

«Удаленный контроль сотрудников клинико-диагностической лаборатории»

Клинико-диагностическая лаборатория (Казахстан) существует с 2003 года и на сегодняшний день является крупнейшей сетью из 13 лабораторных комплексов и многочисленных офисов более чем в 20 городах России. В группе компаний трудится около 2000 сотрудников. 70% из них – офисный персонал. Обратился директор по стратегическому развитию клинико-диагностической лаборатории из Казахстана. Была поставлена задача – контролировать работу сотрудников региональных филиалов удаленно. После внедрения программного обеспечения уже в первую неделю сотрудники осознали, что руководитель (вне зависимости дислокации) контролирует не только задачи и результаты, но и чем конкретно специалисты занимаются за компьютерами в рабочее время. Это поспособствовало росту самомотивации персонала. Сотрудники стали более дисциплинированным, меньше времени проводят в соцсетях и за онлайн-шопингом, больше внимания уделяют своим непосредственным обязанностям. Предложите программно-аппаратное решение.

Рис.11 – Контент соцсетей – иллюстрация по запросу автора выполнена ИИ «Нейроплод».

Задача 4.5.

«Предприимчивый «фрилансер»

Компания клиента занимается разработкой мобильных приложений. В команде более 30 IT-разработчиков, веб-дизайнеров, стратегов и копирайтеров. Чтобы следить за эффективностью работы своего персонала и справедливо начислять заработную плату, в компании использовался тайм-трекер, который следил, чтобы сотрудники занимались работой, а не личными делами.

Один из маркетологов стал показывать низкий результат по привлечению новых клиентов. Однако, тайм-трекер показывал, что его продуктивность на уровне среднего показателя по команде.

Была проведена беседа с сотрудником, но результатов она не принесла - показатели оставались плохими, а он утверждал, что работает на пределе своих возможностей.

Контекст переписок явно указывал на недобросовестные действия со стороны сотрудника - он брал заказы на стороне («фрилансил») в оплачиваемое рабочее время.

Как задокументировать недобросовестные действия работника и обоснованно его наказать или уволить?

Задача 4.6.

«Найти злоумышленника»

Примерно с сентября резко сократился процент продления использования продуктов IT-компании. Отдел контроля качества начал обзванивать клиентов с целью выяснить, кто сделал более выгодное предложение. Бенефициар почти во всех случаях был разный. Кроме того, один из клиентов рассказал, что ему звонили сразу из нескольких организаций. Специалисты компании провели внутреннее расследование и выяснили, что один из сотрудников продает базу.

Как найти злоумышленника? Предложите свои версии.

Задача 4.7.

«Кража интеллектуальной собственности»

Михаил — руководитель компании «Билтех». Предприятие специализируется на разработке, производстве и продаже мониторов, промышленных компьютеров и дисплеев.

Последний год компания занималась разработкой взрывопрочного компьютера, эта инновация могла использоваться во многих сферах, включая ракетостроение. На разработку, испытания и сборку компьютера был потрачен год и около 15 млн. рублей. Один из инженеров «Билтех», уходя из компании, прихватил архив весом около 900 мегабайт, где лежали все чертежи, документы и данные разработки.

Если он продаст эту информацию конкурентам, то помимо 15 млн. руб. «Билтех» потеряет возможную прибыль, так как часть клиентов может купить разработку у конкурентов.

По подсчетам аналитиков компании, недополученная прибыль может достигать около 175 млн. руб.

Плюс ко всему, Михаил заметил, что сроки разработки новых агрегатов стали постоянно сдвигаться, а это грозило компании срывом поставок и потерей прибыли.

Михаил пытался поговорить с руководителями отделов, чтобы выяснить причину срывов дедлайнов, вводил штрафы за просроченные проекты, но ситуация оставалась прежней. Изобретение новых технологий и модернизация текущих сильно затягивались, количество продаж стремительно падало.

Чтобы выяснить причину падения прибыли и не допустить повторения кражи интеллектуальной собственности, Михаил задумался о возможных путях решения.

Предложите комплекс мер по противодействию краже и утечке корпоративной информации.

Задача 4.8.

«Политика безопасности для образовательной организации»

Разработать политику безопасности для конкретной образовательной организации. Определить ответственных лиц за безопасность функционирования информационной системы, их полномочия и ответственность отделов и служб в отношении безопасности. Продумать организацию допуска сотрудников и порядка приема их и увольнения, организацию пропускного режима посетителей. Регламентировать правила разграничения доступа сотрудников к информационным ресурсам. Определить использование программно-технических средств защиты; другие требования общего характера.

Разработка должна быть выполнена в форме комплекта локальных документов.

Задача 4.9

«Работа в условиях пандемии»

В условиях пандемии и вынужденной работы образовательной организации по «удалёнке», обостряется существующая вероятность

потери и повреждения информации как студентами, так и преподавателями и администрацией образовательного учреждения.

Угроза может носить как преднамеренный, так и случайный характер и требование обойтись только лишь повышением информационной культуры участников информационного пространства, тем более, когда они «предоставлены сами себе», не может быть эффективным и гарантированным. Необходимы комплексные меры которые помогут снизить риски относительно безопасности информационных ресурсов.

Предложите наиболее полный перечень таких мер.

Раздел 5. Реальные кейсы.

Источник: https://www.orange-business.com/ru/blogs/chm-po-futbolu-2018-kak-mi-obespechivaem-bezopasnost-i-nadezhnost-seti-vo-vremya-krupnikh.

Кейс №1

Во время карантина к организации, обеспечивающей информационную безопасность обратился банк. Несколько тысяч его сотрудников перешли на удаленную работу. Чтобы ее обеспечить, нужно было значительно расширить пропускную способность интернет-портов, которые использовались для удаленного доступа сотрудников к внутренним ИТ-системам банка. Также важно было обеспечить защиту сервисов от DDoS-атак — банки подвергаются им гораздо чаще остальных компаний. Сделать все нужно было за неделю. Наметили план работ. Чтобы успеть сделать большой объем работы за короткий срок, важно было все правильно распланировать. В течение одного дня мы наметили, какие изменения в сети нужно провести, определили группы специалистов и продумали, как «запараллелить» работы.

В итоге получился такой список:

- Согласовать с клиентом техническое решение, цены, сроки и порядок работ;
- Провести аудит сетевой инфраструктуры на предмет готовности к расширению;
- Организовать агрегированный канал 20G между двумя ключевыми узлами городской сети;

- Выполнить перемонтаж муфт;
- Собрать новые оптические трассы со спрямлением ВОЛС с 60 до 10 км;
- Провести апгрейд сети доступа
- Организовать новые стыки на междугородней телефонной станции М9 (ММТС-9);
- Установить новый сервер URL-фильтрации на М9;
- Установить 10G CPE в стойках клиента в дата-центрах;
- Организовать новые кроссировки в дата-центрах;
- Провести тестирование решения и сдать сервисы клиенту.

На выполнение всех работ потребовалось 4 дня. Были задействованы 12 отделов компании (всего более 50 человек).

Было обновлено оборудование для защиты от DDoS-атак. Не все компоненты сети были готовы обеспечивать пропускную способность в 25 раз выше исходной. В некоторых местах потребовался апгрейд и обновлены стыки с операторами. Скорость передачи данных для клиентов зависит не только от емкости нашей сети, но и от пропускной способности на ее стыках с другими интернет-провайдерами. Было обновлено оборудование в дата-центрах для обеспечения связи и защиты от DDoS-атак. Необходимо было также заменить оборудование в дата-центрах.

Поскольку вся работа была связана с увеличением пропускной способности — для этого требовался существенный апгрейд:

- установить новое оборудование на промежуточных узлах;
- установить новое оборудование в дата-центрах;

- умощнить систему защиты от DDoS-атак, чтобы она поддерживала защиту всей выделенной пропускной способности.

По существующей трассе за 4 дня было сложно провести апгрейд всего оборудования, поэтому было принято решение изменить трассу и сократить, таким образом, количество активного оборудования, так как чем короче трасса — тем выше отказоустойчивость.

В итоге банк вовремя получил нужную скорость основных портов, с надежной защитой сервисов от DDoS-атак.

Кейс №2

Крупный военный завод. На заводе работают порядка 16 000 человек на 5600 автоматизированных рабочих местах (АРМах). Инфраструктура расположена в двух ЦОДах плюс в мобильном ЦОДе. Итого 119 объектов/отделов на 15 площадках.

Начало работ по информационной безопасности 15 июля 2019 года, окончание — 27 декабря 2019 года.

Сложность ИБ-проектов кроется как раз в той самой нормативной базе. Когда требование есть, но реализовать его невозможно, во всяком случае, в рамках текущего времени и бюджета. В противном случае или это требует изменения такого количества процессов в производстве, что вы даже не захотите начинать об этом думать.

В рамках данного проекта подрядчики должны были обеспечить требования следующих нормативных документов (сокращенный перечень):

1. постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

2. приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

3. приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

4. приказ ФСТЭК России от 28.02.2017 № 31 «Об утверждении Требований к обеспечению защиты информации, содержащейся в информационных системах управления производством, используемых организациями оборонно-промышленного комплекса»;

5. приказ ФСТЭК России от 29.05.2009 № 191 «Об утверждении Положения по защите информации при использовании оборудования с числовым программным управлением, предназначенного для обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну»;

6. приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

Система защиты должна была быть аттестована, а потом проверена регуляторами, что очевидным образом максимально повышает приоритет задаче: неукоснительное выполнение требований.

Требования прописаны в государственном контракте, и, несмотря на то, что в данном списке есть неприменимые к заводу нормативно-правовые акты (НПА), их требования необходимо выполнять.

Некоторые НПА предъявляют разные требования к одним и тем же элементам, а, следовательно, реализовывать их надо будет все, т.е., если один НПА предъявляет минимальные требования, а другой – повышенные, реализовывать надо будет по максимуму.

При отсутствии технической возможности выполнения требований, можно применить организационные мероприятия. Но это потребует огромного количества согласований и может растянуться на годы в такой огромной организации, как военный завод, а срок исполнения проекта ограничен.

В случае невозможности реализовать конкретное мероприятие, его можно попробовать согласовать с региональным регулятором. При замене технических мер организационными, если вы точно не укладываетесь в сроки, необходимо подготовить план мероприятий, который может включать:

- Четкие этапы внедрения новых мер.
- Сроки данных этапов.
- Ответственных за выполнение плана.
- Обязательное обучение сотрудников и ответственных.
- Быть принятым на уровне организации.

Все масштабные мероприятия сопряжены с рисками потери связи, крупных DDoS-атак или получением доступа к сетям злоумышленниками, поэтому к таким событиям важно готовиться заранее.

Собрали все риски и выделили самые опасные. Для определения рисков мы собрали команду экспертов — технических специалистов, специалистов по кибербезопасности, по взаимодействию с операторами, органами власти, собственниками зданий, представителями продаж. Команда выделила все риски, которые могли произойти и проверила их по общей методологии.

Каждый эксперт оценил все риски по двум параметрам: вероятность наступления и потенциальный ущерб. Если по каким-то рискам оценки экспертов расходились, проводили дебаты, на которых выясняли, что эксперты могли упустить — и снова оценивали эти риски. Команда выделила все риски, которые могли произойти и проверила их по общей методологии.

Источник: https://www.h-x.technology/ru/case-group/penetration-testing-audit-ru

Кейс №3

Тест на проникновение в режимах «серый ящик» и «белый ящик» телеком-компании.

Телеком-компания среднего размера, мотивированная выполнять внешние требования безопасности, запросила у нас построение комплексной системы защиты информации и проведение общей оценки безопасности. В качестве режимов пентеста заказчиком были выбраны «серый ящик» и «белый ящик». Целевые объекты пентеста: внешние сервера, DMZ, Web-приложения, а также внутренние узлы локальной сети. В ходе проекта были обнаружены следующие уязвимости и недостатки:

- Ошибки конфигурации сети, отсутствие сегментации (отсутствие отдельного VLAN для управляющих интерфейсов устройств iLO, IMPI, IP KVM и т. д.);
- Слабые пароли в активном сетевом оборудовании;
- Доступность скрытых ресурсов (ADMIN$, C$, D$ и др.).

В результате эксплуатации были получены документы, содержащие конфиденциальные данные.

Таким образом, был смоделирован несанкционированный доступ злоумышленников. Заказчик получил исчерпывающий отчёт об уязвимостях и способах их ликвидации, а также перечень мер для предотвращения реализации рисков.

Кейс №4

Анализ кода для мирового производителя техники.

Мировой производитель бытового и промышленного оборудования собирался внедрить новые модули для своих систем ERP, CRM, финансов и электронной коммерции.

Модули были написаны с использованием Java, C ++ и SAP UI5.

Заказчик просканировал исходные коды с помощью сканеров безопасности исходного кода программного обеспечения, выполнил пентест, обнаружил проблемы с безопасностью, исправил их и попросил нас сделать проверку безопасности исходного кода вручную.

Общий объем работы составил около 2 миллионов строк, и примерно через 3 месяца мы представили подробный отчет, показывающий критические проблемы безопасности, которые были пропущены даже сканерами безопасности и даже тестом на проникновение в режиме «серый ящик».

Например, мы обнаружили критические уязвимости состояния гонки, которые могут появляться не часто, но могут нанести огромный ущерб.

Другим примером был бэкдор в программном коде, позволявший разработчикам программного обеспечения получать несанкционированный доступ к производственной системе. Разработчики объяснили, что им нужен этот доступ для законных целей отладки, однако это представляло риск, и мы настояли на закрытии этого бэкдора.

Выводы: заказчик принял правильное решение доверить нам независимую проверку результатов собственных работ по обеспечению безопасности и получил важную информацию по упущениям, которые могли бы на нести серьезный финансовый ущерб. Исправления в системах были выполнены, их безопасность была обеспечена, и риски потерь сведены к минимуму.

Кейс №5.

Тест на проникновение решения DEX и узлов Cardano

Во время теста на проникновение в торговое решение DEX была проведена оценка трёх полных узлов Cardano. Оценка проводилась в режимах "черный ящик" и "серый ящик". В результате было обнаружено, что не установлены 4 обновления безопасности, также были подтверждены 3 уязвимости на уровне ядра. Заказчик устранил обнаруженные уязвимости, после чего начал безопасно выполнять операции по управлению пулом.

Исходный код протокола ликвидности для несгораемых токенов, включая смарт-контракты, был подвергнут аудиту безопасности с использованием сопоставления уязвимостей по схемам классификации CWE/SANS Top 25, DASP Top 10 и SWC Registry. Были обнаружены дорогостоящие циклы, мертвый код, ненадлежащий уровень видимости функций в контрактах и интерфейсах, а также слабые места, на которые потенциально могут повлиять майнеры. Уязвимости были классифицированы как SWC-135, SWC-100, SWC-108 и DASP-8. Заказчик получил подробный

отчет со всеми находками, которые впоследствии были успешно устранены и исправлены в новом релизе.

Кейс №6

Подготовка к расследованиям инцидентов безопасности в банке.

Крупнейший восточноевропейский банк обратился к нам с просьбой помочь удовлетворить требования международной платёжной системы SWIFT. Для этого было необходимо внедрить и протестировать регламент и процедуру реагирования на инциденты информационной безопасности.

Для достижения указанной цели были выполнены следующие задачи:

общие подготовительные работы: согласование с заказчиком регламента расследований на основе существующих политик информационной безопасности заказчика, а также релевантных требований и норм;

подготовка команды экспертов для удалённых расследований и расследований в помещениях заказчика;

подготовка к удалённым расследованиям: настройка удалённого доступа и инструктирование специалистов заказчика;

проведение учебного (тестового) расследования, сценарий тестового инцидента и степень нашего информирования о нём определялись полностью на усмотрение заказчика;

выполнение расследований по мере возникновения реальных инцидентов информационной безопасности, взаимодействие с заказчиком согласно регламенту;

Мы предложили заказчику следующий набор типовых событий и инцидентов безопасности и процедур их обработки:

- Аномальная активность в системе или логах транзакций.
- Компрометация реквизитов доступа (кратковременная).
- Подмена личности (длительная APT атака, разовая атака, разведка и т. д.).
- Повышение привилегий.
- Нарушение зон доступа или разделения ресурсов между критичными и общими ИТ-системами.
- Утечка конфиденциальной или внутренней информации, либо угроза её разглашения.
- Вирусная атака (онсайт или удалённо, в зависимости от последствий и степени поражения).
- Нарушения наблюдаемости, целостности журналов событий и нарушения апеллируемости.
- Другие нарушения целостности (вмешательство или несанкционированное изменение).
- Атака на отказ в обслуживании.
- Другие инциденты.

На протяжении двух месяцев мы разработали и согласовали с заказчиком регламент и процедуры реагирования. После того, как мы выделили ресурсы для реагирования и расследования, заказчик инициировал тестовый инцидент и передал нам дампы памяти и жёсткого диска без каких-либо подробностей по инциденту. "Скомпрометированный" сервер был отключен от сети, и его место занял резервный сервер.

Кейс №7

Внедрение стандарта ISO 27001 для норвежской компании.

К нам обратилась норвежская компания, которая разрабатывает расширения для продуктов и сервисов Microsoft Office, с запросом на соответствие (комплаенс) международному стандарту безопасности ISO 27001. Необходимость этого комплаенса была вызвана тем, что клиенты были обеспокоены вопросами безопасности: насколько безопасно хранить личные данные в расширениях, какие данные хранятся и т. д. Чтобы удовлетворить растущий спрос клиентов на безопасность своих решений, компания решила внедрить стандарт безопасности ISO 27001.

В процессе выбора они обратились к нескольким компаниям, которые занимаются внедрением данного стандарта, и по соотношению цена-качество выбрали в процессе переговоров нашу компанию. Мы предоставили наглядную информативную презентацию, провели несколько созвонов, в ходе которых объяснили наши конкурентные преимущества, а также наш комплексный системный подход.

Мы провели gap analysis в главном офисе заказчика (Осло, Норвегия), в ходе которого были проверены все контроли стандарта ISO 27001 и были выявлены слабые места. Эти пробелы были обусловлены тем, что компания небольшая и многие процессы, в IT и не только (операционные процессы, физическая безопасность и т.д.), не дотягивали до уровня ISO 27001.

Далее мы разработали план внедрения и начали работу по внедрению стандарта. На этапе внедрения мы разработали несколько десятков политик и процессов информационной безопасности. В частности, скорректировали процесс hiring and termination, благодаря которому теперь IT-отдел узнает своевременно о найме и увольнении сотрудников. Это дало возможность своевременно создавать и удалять аккаунты с минимально необходимыми привилегиями. Теперь новые сотрудники получают вводные тренинги по информационной безопасности, а уже в процессе работы – более специализированные тренинги.

Также требования информационной безопасности были внедрены в проекты. При разработке проектов учитываются вопросы защиты информации, проводится анализ рисков и выполняются все остальные требования стандарта безопасности ISO 27001.

Обычно в других компаниях анализ взаимодействия с третьими сторонами – это отдельная большая работа. Здесь же эта работа была сведена к минимуму, поскольку для всех целей используются только продукты и онлайн-сервисы компании Microsoft, у которой есть полный набор сертификатов по безопасности, включая ISO 27001, VDA ISA, SOC 2 и т. д.

Процесс согласования внедрения новых документов проходил гладко, без лишних формальностей и бюрократии. Далее сотрудники прошли тренинги, и политики начали работать.

После того, как процесс внедрения был закончен, мы приступили к выбору независимого сертификационного аудитора. Вот здесь мы столкнулись со сложностями, вызванными очень

медленным ответом аудиторов. Возможно, это было связано с карантином или с сезонными пиками. Ответа одного из аудиторов мы ждали несколько месяцев, а от второго вообще не дождались. Поэтому мы нашли третью аудиторскую компанию, которая является представительством немецкого сертификационного органа, аккредитованного DAkkS.

В результате клиент успешно прошёл независимый аудит и получил официальный сертификат ISO 27001.

На протяжении одной рабочей недели мы проанализировали дампы и обнаружили тестовое заражение компьютерным вирусом. Мы выполнили обратную инженерию и разработали полный отчёт, в котором показали заказчику способ и ход заражения, а также сделали вывод об опасности вируса и дали рекомендации по его удалению.

Заказчик остался доволен нашей работой, отчитался перед SWIFT и приобрёл годовую подписку на нашу услугу управляемого реагирования на инциденты безопасности. Затем мы предложили заказчику наши услуги внедрения PCI DSS, но это уже другая история.

Кейс №8

Внедрение центра безопасности (SOC) и системы управления событиями безопасности SIEM в банке.

Банк средней величины обратился к нам с целью внедрения SIEM в их собственном дата-центре. Этот банк имел некоторые элементы центра операций по безопасности (SOC), и попросил нас

усовершенствовать его, привести к современным стандартам и взять на себя его поддержку.

Из нескольких доступных моделей SOC/SIEM (on-premise SOC, облачное внедрение, полный аутсорсинг и т. д.), клиентом была выбрана комбинированная модель, предусматривавшая работу нашего персонала с системами мониторинга, физически находящимся в банке.

Вначале мы провели инвентаризацию информационных активов клиента, определили источники событий от более чем 5000 хостов , расположенных в 12 офисах и дата-центрах банка, в том числе более 50 серверов баз данных. Далее мы определили профили инцидентов, процедуры реагирования и поддержки, а также оценили ёмкость потока инцидентов, которая составила около 1500 EPS.

На базе кластера высокой доступности IBM QRadar в дата-центре банка мы реализовали следующие функции и компоненты: управление журналами, управление событиями безопасности, аналитику угроз, управление рисками и уязвимостями, анализ поведения пользователя и сущностей, машинное обучение, оркестровку и реагирование, приманки и поиск угроз, цифровую криминалистику.

Наши специалисты разработали правила и процедуры, написали недостающие кастомные парсеры и оперативно подключили источники событий от Microsoft Server Family, Microsoft System Center, RedHat Enterprise Linux, Hitachi, IBM AIX, IBM Storage Manager, Cisco IOS/NX-OS, Check Point NGX, SAP, Citrix XenServer,

XenDesktop, XenApp, Microsoft SQL, Oracle, Microsoft Exchange, SharePoint, UAG и многих других типов систем.

Мы защитили компоненты системы файрволами, а потоки данных – Site-to-Site VPN, определили матрицы ролевого доступа к системе, настроили непрерывное обновление, а также выполнили тонкую настройку правил и протестировали определение аномалий и угроз.

Непосредственно перед переводом в продакшн мы распределили роли и обязанности по безопасности между нашим персоналом и штатом заказчика, провели его обучение и запустили систему в промышленную эксплуатацию.

Внедрение системы заняло у нас 8 месяцев.

Выводы: в результате внедрения банк получил современный центр безопасности на базе системы мониторинга событий и реагирования на угрозы безопасности в реальном времени. Кроме прочего, мы оптимизировали некоторые технологические процессы заказчика, обнаружили устаревшие активы, улучшили управление доступом к серверам, наладили сбор и хранение протоколов событий безопасности в соответствии с требованиями PCI DSS и национальными требованиями к сбору доказательств, приемлемых в суде. Банк успешно прошёл несколько внешних независимых аудитов и выполнил требования соответствия нормам и стандартам. Общий годовой ущерб от инцидентов безопасности снизился в несколько раз.

Источник: https://www.jetinfo.ru/5-kejsov-jet-cybercamp

Кейс 9

По данным Check Point, в 2021 г. кибератак стало на 40% больше, чем в 2020-м (в России — на 54% больше). В среднем, каждую неделю хакеры совершали 1153 нападения. Целевые атаки растут пропорционально. Они долго и тщательно планируются и часто основаны на инсайдерской информации. На их реализацию хакерские группировки закладывают от трех месяцев и более. В большинстве случаев злоумышленникам противостоят команды SOC. Проблема в том, что специалисты центров в основном сталкиваются со штатными угрозами, эксплуатацией общеизвестных уязвимостей и скрипт-кидди. У многих из них просто нет опыта работы со сложными, многоступенчатыми атаками, ведь его можно получить только в бою (как говорится, вам нужен опыт работы для первого места работы). Что с этим делать? Отправить ИБ-специалистов на киберучения.

На платформе Jet CyberCamp можно научиться противостоять разным видам атак. Для организации киберучений наши эксперты изучают громкие инциденты и актуальные уязвимости. Затем разрабатывают сценарий, состоящий из цепочки действий злоумышленников — от проникновения в сеть до установки майнера или кражи базы. В результате участники могут отработать навыки расследования и реагирования на инциденты в условиях, близких к реальным.

Изначально Jet CyberCamp закрывал внутренние потребности Jet Security Team. На небольшой инфраструктуре пентестеры исследовали новые уязвимости, а инженеры и специалисты SOC противостояли кибератакам. По мере развития платформа обрастала контентом: мы структурировали знания, создавали гайды по работе с СЗИ и процессами расследования инцидентов. В результате Jet CyberCamp превратился в полноценную площадку для киберучений с развитой инфраструктурой, множеством средств защиты, сильным теоретическим и практическим блоком. Теперь на ней тренируются не только Jet Security Team, но и наши заказчики и партнеры.

Кроме того, платформа включает функционал, позволяющий отслеживать успешность обучения, проверять полученные навыки и выявлять слабые и сильные стороны специалистов. Все это позволяет использовать Jet CyberCamp для решения самых разных бизнес-задач. Ниже приведем пять кейсов использования платформы.

Одна из ключевых задач Jet CyberCamp — регулярная прокачка практических навыков ИБ-специалистов. Мы готовы делиться опытом Jet Security Team, рассказывать об актуальных угрозах, ярких кейсах и лучших практиках защиты. Для этого мы регулярно дополняем платформу свежими сценариями, в основе которых лежат кейсы, с которыми сталкиваются специалисты «Инфосистемы Джет».

Кейс № 9.1: наем сотрудников.

Компании А нужно регулярно находить новых специалистов первой линии SOC. Это связано с большим географически распределенным штатом и высокой текучкой на этой позиции. Люди

не задерживаются на месте — случается и рост, и разочарование в работе. В целом задача решается на уровне филиалов, где для поиска и обучения специалистов первой линии выделены отдельные сотрудники.

Решение: проводим один из этапов собеседования в формате киберучений. Формируем для соискателей сценарии, не требующие глубоких навыков работы со средствами защиты, но выявляющие их сильные и слабые стороны. На платформе доступны сами сценарии, тесты до и после обучения, а также раздел Wiki с гайдами по СЗИ.

Компания оперативно получает информацию о прогрессе соискателей, оценивает их аналитические способности и навыки работы с большим объемом информации. Это помогает эффективнее отсеивать незаинтересованных соискателей и ускоряет интеграцию новичков в рабочий процесс. Кроме того, так проще выявлять специалистов, предрасположенных к работе с инцидентами.

Кейс № 9.2: прокачка и карьерный рост специалистов.

Компания Б решает другую задачу: массовое стремление специалистов первой линии SOC перейти на вторую линию. Опять же, сотрудники редко задерживаются на своих местах — это связано и с монотонностью работы, и с интересом к новым вызовам. При этом далеко не все сотрудники, переходящие на вторую линию, остаются довольны — их представления о работе не всегда соответствуют действительности.

Решение: тренируем в Jet CyberCamp специалистов первой линии и проверяем, готовы ли они к переходу на вторую. Для этого

формируем годовой план обучения, основанный на реальных кейсах второй линии. Во время тренировок действия каждого специалиста анализируются: учитываются результаты тестов, скорость прохождения сценариев, частота обращения к платформе и эффективность работы со средствами защиты.

В результате сотрудники могут поработать с реальными задачами второй линии и решить, насколько им подходит эта роль. Некоторые понимают, что сначала им нужно подтянуть теорию и практические навыки. А те, кто успешно справляются с обучением, переходят на новую позицию и быстрее интегрируются в рабочий процесс.

Платформа помогает компании выявлять талантливых специалистов, которые засиделись на месте, и предоставляет прозрачный путь развития для всех, кто стремится к профессиональному росту. Кроме того, проект положительно влияет на общий уровень лояльности сотрудников.

Во время киберучений мы анализируем прогресс обучающихся по результатам выполнения разных задач. Например, учитываем скорость обнаружения флагов или написания верных правил. Для каждой тренировки выделены техники по матрице MITRE. Сценарии составлены так, чтобы при прохождении годового плана специалисты поработали со всеми актуальными техниками.

Кейс № 9.3: выбор продукта в рамках импортозамещения.

Компания В не была ограничена в выборе СЗИ и в основном пользовалась продукцией западных вендоров. Но согласно указу

Президента РФ от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» большую часть зарубежных решений нужно заменить на отечественные аналоги. Помимо кадровой проблемы (специалисты привыкли работать с западными продуктами) перед компанией встала задача выбора эффективных отечественных аналогов.

Решение: здесь Jet CyberCamp выступает в роли площадки для демонстрации средств защиты. Как правило, демостенды оторваны от реальной инфраструктуры и демонстрируют уязвимости в вакууме. Например, работа антивируса показывается в отрыве от SIEM. Кроме того, чтобы протестировать решения разных вендоров, нужно провести массу встреч. Киберполигон же позволяет централизованно и наглядно увидеть совместную работу разных средств защиты.

Для решения задачи можно разработать сценарий атаки, основанный на реальном опыте ИБ-специалистов компании В: они тестируют СЗИ одного класса от разных вендоров и выбирают подходящие решения. Дополнительно мы проводим комплексные киберучения (в том числе с участием вендоров), чтобы сотрудники быстрее познакомились с новыми инструментами.

Кейс №9.4: отработка плейбука и взаимодействие в команде.

Компании Г удалось предотвратить серьезную кибератаку, но буквально в последний момент. Ее редко атакуют, ИБ-специалисты почти не сталкиваются со сложными вызовами, поэтому им банально не хватает практического опыта. При встрече с реальной угрозой они начинают штудировать внутренние регламенты, а не реагируют на инцидент. Кроме того, сотрудники не до конца понимают свою роль в

команде, что ведет к простоям и дублированию активностей или работе не по плейбуку.

Решение: для компании Г уместно проведение классических киберучений, включающих прокачку навыков командной работы и расследования инцидентов. Основная цель — наработка опыта на релевантных кейсах и отработка существующего плейбука.

Кейс № 9.5: стресс-тесты и проверка знаний сотрудников.

ИБ-специалисты компании Д часто сталкиваются с угрозами, но большинство из них достаточно просты: фишинговые письма, атаки на портал и подозрительная активность пользователей, которая имеет логическое объяснение. Но даже такие кейсы могут вывести специалистов SOC из строя. Причин две: плохо выстроенные процессы и трудности при работе с большим объемом данных.

Сотрудникам компании сложно приоритизировать задачи. Они признают, что не успевают и не знают, в каком порядке нужно реагировать на инциденты. И, как в прошлом кейсе, не все специалисты четко осознают свою зону ответственности. Один из показательных инцидентов: при очередной фишинговой рассылке один из технических специалистов поддался панике и написал письмо на всех ИБ-коллег с темой «Нас ломают!». После этого о работе по плейбуку речи не шло.

Решение: компании Д подходит годовая программа тренировок, включающая стресс-тесты и прокачку навыков командной работы. В ходе киберучений анализируем скорость прохождения сценариев и роли, которые выбирают для себя специалисты. Основная цель — улучшить навыки реагирования на инциденты и проверить знания о лучших практиках расследований.

Раздел 6. Разработка кейс-задач.

Структура кейс-заданий зависит от вида кейса и его целей. Но в самом общем виде кейсовое задание состоит из вводной, основной и завершающей частей.

Вводная часть – дает общую информацию о «кейсе». Она может содержать «вызов» – небольшое вступление, предисловие, интригующее задачерешателя.

Существуют следующие варианты предисловия: определенная сюжетная завязка, которая вызовет интерес к рассматриваемой ситуации; исходные данные исследования, глоссарий терминов, ключевые моменты; формулировка вопросов для исследования и т.п. В вводной части может излагаться гипотеза, которую нужно подтвердить или опровергнуть в процессе решения кейса.

Основная часть – контекст, случай, проблема, факты.

Завершающая часть или материалы для решения представляет дополнительную информацию, которая позволит лучше разобраться в «кейсе»: вопросы, библиография, фотографии персонажей, схемы, таблицы.

Текст кейса может быть различным по объему. Различают полные кейсы, сжатые кейсы и мини-кейсы.

Полные кейсы (в среднем 20–25 страниц) предназначены для командной работы в течение нескольких дней и обычно подразумевают командное выступление для презентации своего решения.

Сжатые кейсы (3–5 страниц) предназначены для разбора непосредственно на занятии и подразумевают общую дискуссию.

Мини-кейсы (1–2 страницы и менее), как и сжатые кейсы, предназначены для разбора в аудитории и зачастую используются в качестве иллюстрации к теории, преподаваемой на занятии.

Пользуясь приведенной таблицей, составить кейс-задачи по тематике использования информационно-коммуникационных технологий в образовании, либо по информационной безопасности в образовательных организациях.

Таблица 1. Типы кейсов, способы их представления

Типы кейсов (Гарвардская школа)	**Способ представления**	**Создание проблемной ситуации**	**Подготовка кейса**	**Содержание кейса**	**Выбор создание итогового решения**
Обучающий кейс (Case-stated method). Stated-установленный, зафиксированный	Иллюстративные учебные ситуации-кейсы, цель которых – на определенном практическом примере обучить алгоритму принятия правильного решения в определенной ситуации	Преподаватель задает, определяет проблему	Педагог готовит кейс	Кейс содержит 2-3 готовых варианта решения по рассматриваемой проблеме	Обучающимся предлагается высказать свои мнения.
Аналитический кейс (информационный) (Case-incident method). Incident-присущий, свойственный, связанный	учебные ситуации – кейсы с формированием проблемы, в которых описывается учебная (условная) ситуация в конкретный период времени, выявляются и четко формулируются проблемы. Цель такого кейса –	Преподаватель задает, определяет проблему	Педагог готовит кейс	Кейс содержит несколько вариантов (3-4) решения и некоторое количество информационных источников	Обучающиеся должны выбрать вариант решения и обосновать его, опираясь на материалы готового

	диагностирование ситуации и самостоятельное принятие решения по указанной проблеме			по рассматриваемой проблеме	кейса
Эвристический кейс (Case-problem method). Problem-проблема, проблемная ситуация	прикладные упражнения, в которых описывается конкретная сложившаяся ситуация, предлагается найти пути выхода из нее; цель такого кейса – поиск путей решения проблемы.	Преподаватель определяет проблему в общих чертах, обучающиеся конкретизируют проблему (для младших школьников конкретизацию проблемы может также осуществить преподаватель)	Преподаватель готовит начальный кейс. Обучающиеся его дополняют, при необходимости	Кейс содержит некоторое количество информационных источников по рассматриваемой проблеме, может содержать некоторые варианты решений, иллюстрирующие примеры и пр.	Обучающиеся должны выстроить собственное обоснованное решение, опираясь на материалы готового кейса. Возможно, для обоснования своей точки зрения, обучающиеся дополняют кейс новой информацией
Исследовательский кейс (Case-study method). Study-исследование	учебные ситуации – кейсы без формулирования проблемы, в которых описывается более сложная, ситуация, где проблема четко не выявлена, а представлена в статистических данных, оценках общественного мнения, органов власти и т.д. Цель такого кейса –	Преподаватель определяет проблемное направление, обучающиеся самостоятельно задают проблему (младшим школьникам	Преподаватель готовит начальный кейс, обучающиеся его дополняют	Кейс содержит некоторое количество информационных текстов по рассматриваемой проблеме	Обучающиеся предлагают собственное решение. Для обоснования своей точки либо дополняют готовый кейс новой информаци

	самостоятельно выявить проблему, указать альтернативные пути ее решения с анализом наличных ресурсов	необходимо помочь в формулировке проблемы)			ей, либо, в зависимости от решения, готовят новый кейс

Пример выполнения.

1. Обучающий кейс (Case-stated method). Stated установленный, зафиксированный.

Кейс «Рекламное агентство»

Цель кейса – закрепить навыки практической работы с изображениями в текстовом редакторе, поиск в сети Интернет.

Тип кейса – обучающий кейс.

Задание подгруппам: Вы – сотрудники рекламного агентства, отвечающие за разработку рекламных листовок. В ваше агентство пришел клиент – Директор колледжа, которому необходимо разработать агитационную листовку для будущих студентов, чтобы они выбрали именно этот колледж.

Содержание кейса:

– задание 1: Исследование сайтов рекламных агентств, для создания макета рекламной листовки.

– задание 2: Создание макета рекламной листовки в бумажном варианте.

– задание 3: Изготовление листовки за компьютером, для представления своей группе.

Вопросы для обсуждения по материалам кейсов:

1. В группе обсудите: какой вы представляете листовку. Какие функции текстового редактора нужно будет использовать для создания листовки.

2. Опираясь на материалы кейса, определите какие изображения и какой текст будет находиться на вашей листовке.

3. Изготовьте макет листовки в бумажном варианте. Выберете, кто из группы будет реализовывать макет за компьютером, а кого вы назначаете ответственным для презентации вашей листовки.

4. Подготовьте листовку и презентацию для вашего клиента, чтобы убедить его в правильности выполненной вами работы.

Материал кейса

Часть 1

Рекламное агентство — это коллектив творческих людей, которые с помощью средств массовой информации (коммуникационных каналов) осуществляют рекламу (продвижение) услуг или товаров клиента путем привлечения к нему дополнительного интереса.

Что такое листовка? Виды печати листовок. В нашем информационном веке просто невозможно представить проморекламу без использования одного из ее самых эффективных средств – листовки. Сегодня применение листовок имеет широкую сферу. Эта полиграфическая продукция стала одним из самых популярных средств распространения информации. Маленькая листовка оказалась мощным и эффективным инструментом рекламы.

Как выглядит листовка? Она представляет собой печатный лист небольшого размера, на котором размещается изображение или текст агитационного или рекламного характера. Листовки очень выгодны благодаря низкой себестоимости даже при больших тиражах, имеют кратковременную актуальность, быстро печатаются и распространяются. Это делает возможным их использование в любых сферах бизнеса. Чаще всего листовки эффективно используют в целях рекламы, но не только в рекламе они нашли свое применение. Например, в наши дни нельзя представить предвыборную кампанию без использования агитационной листовки. Поэтому печать листовок так востребована и актуальна.

Главная цель рекламной листовки – это рекламирование товаров или услуг, быстрое донесение до потребителя рекламной информации. Очень эффективны листовки во время всевозможных промоакций или больших презентаций, для рекламы новых товаров или услуг. Также, если необходимо привлечение внимания потенциальных клиентов к уже не новым товарам или услугам, листовки сослужат великолепную службу.

Часть 2.

Выполнение студентами практической работы. Обучающиеся изучают сайты рекламных агентств, для создания макета рекламной листовок. Затем создают макет рекламной листовки в бумажном варианте и изготавливают листовки за компьютером, для представления своей группе.

Обучающимся предлагается высказать свои мнения.

2. Аналитический кейс (Case-incident method). Incident - присущий, свойственный.

Кейс «Диаграммы и графики продаж»

Цель кейса – закрепить навыки практической работы в текстовом редакторе и электронных таблицах по созданию организационных диаграмм.

Тип кейса – аналитический кейс.

Задание подгруппам:

Каждая группа – это небольшая фирма, сотрудники которой: менеджер по продажам, менеджер по рекламе и менеджер по кадрам. Вас пригласили инвесторы, чтобы выбрать одну из фирм, для дальнейшего финансирования. Представьте свою фирму с помощью графиков и диаграмм в выигрышном свете.

Содержание кейса:

– задание 1: Исследование материала по видам диаграмм и работе менеджера.

– задание 2: Подготовка деятельности фирмы (в бумажном варианте) и диаграмм за компьютером.

– задание 3: Представление инвесторам презентации своей фирмы с диаграммами.

Материалы кейса:

Часть 1: Диаграммы и их виды.

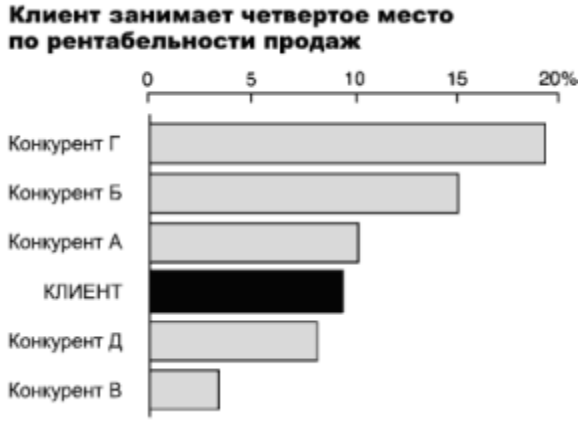
Несмотря на разнообразие графических средств, используемых в различных видах коммуникации (таблицы, схемы, графики,

матрицы и карты), при иллюстрации количественных данных применяется пять основных типов диаграмм:

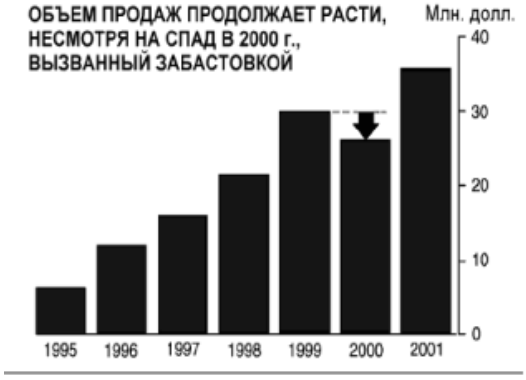
Для того чтобы правильно выбрать тип диаграммы, вы в первую очередь должны четко сформулировать конкретную идею, которую вы хотите донести до аудитории при помощи диаграммы.

Для построения большинства круговых диаграмм лучше использовать не более шести компонентов. Если вам нужно отобразить большее число компонентов, выберите из них пять наиболее важных, а остальные сгруппируйте в категорию «прочие».

При составлении линейчатых диаграмм необходимо убедиться, что пространство, разделяющее линейки, меньше, чем ширина самих линеек. Используйте самый контрастный цвет или штриховку для того, чтобы выделить самый важный элемент, подчеркивая, таким образом, вашу основную идею, выраженную в заголовке.



Советы по подготовке линейчатых диаграмм равным образом относятся и к гистограммам: расстояние между колонками должно быть меньше, чем ширина самих колонок; используйте цвет или штриховку для того, чтобы выделить какой-то момент времени или разграничить данные за прошлые периоды и прогнозные величины.



Без сомнения, из всех типов диаграмм график используется наиболее часто, и это вполне оправданно. Во первых, его легче всего нарисовать. Во вторых, это самый компактный из всех типов диаграмм. Наконец, на графике наиболее наглядным образом можно показать, что значение определенного параметра растет, уменьшается, изменяется или остается стабильным.

Часть 2:

Менеджер - это человек, постоянно осуществляющий управление тем или иным процессом. Основной деятельностью менеджера является анализ, построенный на методах сравнения отчетных и плановых показателей. Диаграмма – лучший способ выражения результатов этой деятельности.

Виды показателей работы предприятия:

– экономические;

– финансовые;

– кадровые;

– производственные.

Обучающиеся исследуют материала по видам диаграмм и работе менеджера. Затем осуществляют подготовку деятельности фирмы (в бумажном варианте) и диаграмм за компьютером. Далее представление инвесторам презентации своей фирмы с диаграммами и графиками. Обучающиеся должны выбрать вариант решения и обосновать его, опираясь на материалы готового кейса.

3. Эвристический кейс (Case-problem method). Problem - проблема, проблемная ситуация.

Кейс «Лицензионный диск или подделка»

Цель кейса – закрепить навыки практической работы с информационными носителями.

Тип кейса – эвристический кейс.

Задание подгруппам:

Исследователи продемонстрировали простой и недорогой способ проверки подлинности товаров на оптических носителях. Установить происхождение компакт-дисков помогло понимание технологии их изготовления и простая лазерная указка. Отличить пиратский CD от лицензионного по внешнему виду невозможно, ведь имитация фабричной упаковки и голографических наклеек весьма качественна. Само явление дифракции и помогло ученым признать разницу между дисками. Представьте себя учеными и объясните характерные отличия между этими двумя дисками.

Содержание кейса:

– задание 1: Исследование дисков с помощью лазерной указки.

– задание 2: Подготовка выводов о проведенном опыте.

Вопросы для обсуждения по материалам кейсов:

1. В группе просмотрите несколько дисков.

2. Определите, какие диски лицензионные, опираясь на материалы кейса

3. Сформулируйте выводы о проделанном эксперименте, разработайте рекомендации по результатам работы.

Материалы кейса:

Часть 1:

Дифракция света.

Если на пути волны возникает препятствие, то происходит дифракция — отклонение волны от прямолинейного распространения. Это отклонение не сводится к отражению или преломлению, а также искривлению хода лучей вследствие изменения показателя преломления среды. Дифракция состоит в том, что волна огибает край препятствия и заходит в область геометрической тени. Пусть, например, плоская волна падает на экран с достаточно узкой щелью. На выходе из щели возникает расходящаяся волна, и эта расходимость усиливается с уменьшением ширины щели.

Вообще, дифракционные явления выражены тем отчётливей, чем мельче препятствие. Наиболее существенна дифракция в тех случаях, когда размер препятствия меньше или порядка длины волны. Дифракция, как и интерференция, свойственна всем видам волн — механическим и электромагнитным. Видимый свет есть частный случай электромагнитных волн; неудивительно поэтому, что можно наблюдать дифракцию света. В результате прохождения лазерного луча сквозь небольшое отверстие диаметром 0,2 мм мы видим, как и полагается, центральное яркое пятно; совсем далеко от пятна расположена тёмная область — геометрическая тень. Но вокруг центрального пятна — вместо чёткой границы света и тени! — идут чередующиеся светлые и тёмные кольца. Чем дальше от центра, тем

менее яркими становятся светлые кольца; они постепенно исчезают в области тени.

Часть 2:

Отличить контрафактный CD от лицензионного по внешнему виду иногда бывает затруднительно. Пираты могут позволить себе весьма качественную имитацию фабричных упаковок и голографических наклеек. До недавнего времени решить этот вопрос можно было только обратившись к эксперту, обладающему необходимым оборудованием. Однако пятеро физиков-оптиков из Университета Гренады (Испания) утверждают, что нашли более простой, но не менее точный способ установить происхождение компакт-дисков. Им помогло понимание технологии изготовления носителей и простая лазерная указка.

Микроструктуры поверхности пиратских и лицензионных дисков имеют характерные отличия. Дело в том, что оригинальные диски производятся на заводах в большом количестве с помощью специального гидравлического пресса, тогда как пиратская продукция выжигается лазером поодиночке на устройствах чтения-записи. Оригинальные диски имеют микроскопические углубления, выдавленные в поликарбонатной основе. Их поверхность покрыта ровным слоем защитного лака. Лазер плеера, проникая сквозь ровный слой защитного лака, воспринимает углубления как звуковые или видеосигналы. В свою очередь, диски, записанные в приводе CD/DVD, не имеют углублений: запись производится путем изменения коэффициента отражения материала – лазер словно

выжигает поверхность диска. Поэтому дифракция световых волн на лицензионном и пиратском дисках заметно различается.

Ученые утверждают, что повторили свой эксперимент более ста раз с дисками разных производителей, и результат оставался неизменным. По заявлению Хавьера Фернандеса-Андреса (Javier Hernandez-Andres), одного из авторов исследования, метод «абсолютно надежен».

Обучающиеся знакомятся с материалом кейса. Затем проводят исследование дисков с помощью лазерной указки и подготавливают выводы о проведенном опыте. Также учащимся необходимо сформулировать выводы о проделанном эксперименте, разработать рекомендации по результатам работы.

Обучающиеся предлагают собственное решение. Для обоснования своей точки либо дополняют готовый кейс новой информацией, либо, в зависимости от решения.

4. Исследовательский кейс (Case-study method). Study-исследование.

Кейс «Магазин компьютерной техники»

Цель кейса – закрепить навыки работы с периферийными устройствами компьютера и навыки практической работы с операционной системой, с элементом панели управления (диспетчером устройств).

Тип кейса – исследовательский кейс.

Задание подгруппам: Ваша группа – сотрудники магазина компьютерной техники. Распределите роли: техник по сбору

компьютера и комплектующих, продавец компьютерной техники, администратор магазина и покупатель.

Ваша задача – собрать оптимальный компьютер по характеристикам и представить покупателю презентацию своего опыта.

Содержание кейса:

– задание 1: Исследование сайтов и прайсов магазинов компьютеров и комплектующих.

– задание 2: Работа с компьютерной техникой (разобранный компьютер), для создания образца.

– задание 3: Представление покупателям готового образца.

Материалы кейса:

1. Прайс-лист магазина компьютерной и бытовой техники «Ситилинк». Сайт компании расположен по адресу: www.citilink.ru.

2. Прайс-лист магазина компьютерной и бытовой техники «ДНС». Сайт компании расположен по адресу: https://www.dns-shop.ru

1. Учащиеся проводят самостоятельное исследование сайтов и прайсов магазинов компьютеров и комплектующих.

2. Проводят работу с компьютерной техникой (разобранный компьютер), для создания образца.

3. Представляют покупателям готовый образец.

Обучающиеся предлагают собственное решение. Для обоснования своей точки либо дополняют готовый кейс новой информацией, либо, в зависимости от решения, готовят новый кейс.

Некоторые варианты решений.

Решение к задаче 1.18

1. Деньги перечислять ни в коем случае нельзя, деньги уйдут, а экран так и будет заблокирован.

2. Этот тип вируса называется «вымогатели». К ним относятся Винлокеры (winlocker - WinLock - программа для ограничения времени работы с Windows. Автоматически загружается при включении компьютера и проверяет время работы. После истечения установленного периода времени WinLock выключает систему). Программа полностью блокирует доступ к компьютеру и требует деньги за разблокировку, на пример положить на счет или тд.

3. Для решения проблемы стоит обратиться на сайт компании Drweb, там можно найти как разблокировать многие винлокеры, за счет ввода определенного кода или выполнения некоторых действий.

4. Для профилактики стоит чаще обновлять антивирусные программы, чтобы они всегда были в рабочем состоянии и последней версии, а также не стоит скачивать подозрительные файлы с непроверенных сайтов.

Решение к задаче 1.19

1. Торрент-файл был заражен трояном. По этой причине начали устанавливаться сторонние приложения.

2. Скачивать файлы только из проверенных источников. В этой ситуации Пете следовало подумать о том, чтобы купить лицензионную версию игры. Также не стоит отключать антивирус.

3.Так как удалить приложения не получается, следует зайти в свойства приложения и во вкладке «безопасность» поставить галочки «разрешить» напротив своего пользователя. Также можно скачать стороннее приложение для удаления программ и с помощью него попробовать удалить приложения.

4. Если этот способ не сработал, то можно обратиться за помощью в интернет. Далее следует убрать из автозапуска службу, которая появилась после установки игры.

5. Включить антивирус и с помощью него найти и удалить вирусы. Если он не нашел вирусов, скачать программу, которая находит вирусы в реестре (например, HijackThis. В интернете есть инструкции как пользоваться этой программой) и вручную удалить вирусы.

6. Удалить рекламные вирусы можно с помощью AdwCleaner (инструкции также есть в интернете). Если антивирус не до конца удалил вирусы, то можно воспользоваться программой Malwarebytes Anti-malware. Перезагрузить компьютер после удаления всех вирусов.

7. Покупать лицензионные игры и приложения; иметь хороший антивирус; не отключать антивирус; не скачивать подозрительные файлы; перед установкой программ читать правила их использования, а также все сообщения, которые программа будет Вам показывать.

Решение к задаче 2.16

1. В первую очередь сотрудник подразделения объектового режима должен сообщить в подразделение информационной безопасности. Затем составить акт добровольной передачи

машинного носителя информации (далее – МНИ), в котором указать номера МНИ, его владельца, обстоятельства передачи и пр.

2. Сотрудник подразделения информационной безопасности вместе с владельцем МНИ следуют в отдел информационной безопасности, чтобы провести анализ находящейся на флешке информации. В ходе анализа становится известно, что на МНИ содержатся файлы (чертежи), составляющие коммерческую тайну предприятия.

3. С сотрудника берётся объяснение, с какой целью он скопировал данную информацию на личный носитель информации и каким образом он сделал это. Сотрудник отказывается давать объяснение, мотивируя тем, что флеш-накопитель лежал у него на рабочем месте без присмотра и любой из его коллег мог скопировать данную информацию на носитель.

4. После беседы с нарушителем, сотрудник подразделения информационной безопасности производит осмотр рабочего места нарушителя, в ходе которого выясняется, что:

- программное обеспечение, предназначенное для защиты информации на данном ПК не установлено
- на ПК не установлен пароль(что противоречит регламенту защиты информации, введённому на предприятии)
- оформление окон в оперативной системе отличается от стандартного, устанавливаемого на предприятии

Всё это даёт основание полагать, что данная операционная система была установлена самовольно, без уведомления сотрудников отдела информационной безопасности.

5. В сотрудничестве с отделом информационных технологий удаётся узнать, что регламентные работы проводились в отделе нарушителя 4 месяца назад и все копии операционной системы были без изменения, а также, все средства защиты информации были настроены таким образом, чтобы исключить попытки подключения незарегистрированного МНИ, а также установку иного ПО.

6. Анализируя содержимое МНИ нарушителя удаётся понять, что он также является загрузочной флешкой.

7. Производится дополнительный анализ рабочего ПК нарушителя, выясняется, что операционная система была установлена месяц назад, а также, что пользователь копировал чертежи перспективных разработок. В сотрудничестве с начальником отдела удаётся узнать, что полтора месяца назад после отказа в выплате премии, у нарушителя ухудшились показатели работы и пропала мотивация. Неделю назад данный сотрудник написал заявление об увольнении.

8. Анализируя данные факты сотрудник подразделения информационной безопасности пишет развёрнутый доклад, в котором указывает факт нарушения, обстоятельства обнаружения МНИ, факт несанкционированной установки программного обеспечения на ПК, факт копирования информации, составляющей коммерческую тайну предприятия, включая ту информацию, работа с которой не входит в обязанности данного сотрудника, а также со слов начальника отдела указывает то, что нарушитель планирует увольняться и, вероятно, хотел забрать данные наработки с собой. К отчёту сотрудник прилагает акт передачи МНИ, письменные объяснения данного

сотрудника, скриншоты с ПК нарушителя, где указана дата установки данной операционной системы, акт осмотра МНИ и отдаёт на рассмотрение заместителю директора по безопасности.

Выводы: Сотрудник пронёс с собой на работу загрузочную флешку и до загрузки операционной системы (далее – ОС), вместе с программными средствами защиты информации произвёл установку ОС, тем самым получив доступ к рабочему ПК. Затем, с других зарегистрированных флешек перенёс на свой ПК информацию, составляющую коммерческую тайну предприятия и перенёс данные на свою флешку с целью на новом месте работы получить за это материальную выгоду. Данный факт оказался возможен благодаря низкому контролю со стороны начальника отдела, а также из-за несовершенства программных средств защиты информации.

Решение к задаче 3.1.

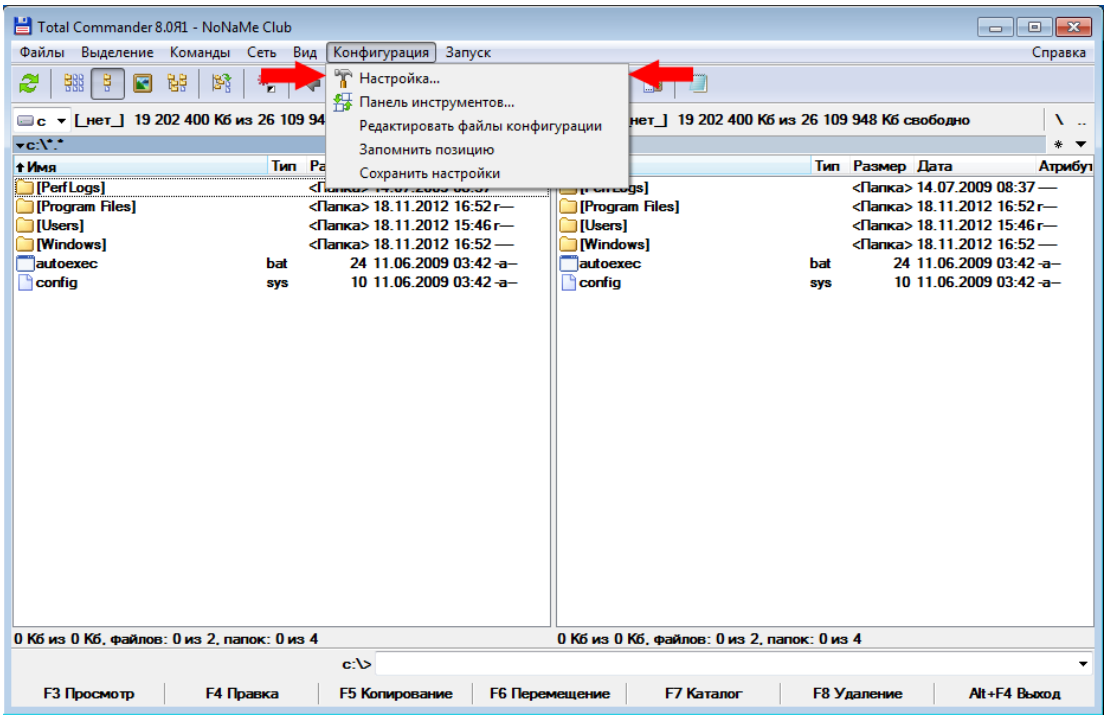
1. Очевидно, что ярлыки, появившиеся на usb-накопителе вместо файлов это вирус, который был подхвачен пользователем на ПК, где он работал.

2. Для того что бы восстановить файлы на накопителе необходимо выполнить следующее.

Например, мы устанавливаем на свой домашний ПК программу Total Commander, и выполняем восстановление файлов по примеру как показано ниже

А. Запускаете программу: *Настройка программы для отображение скрытых папок (файлов);*

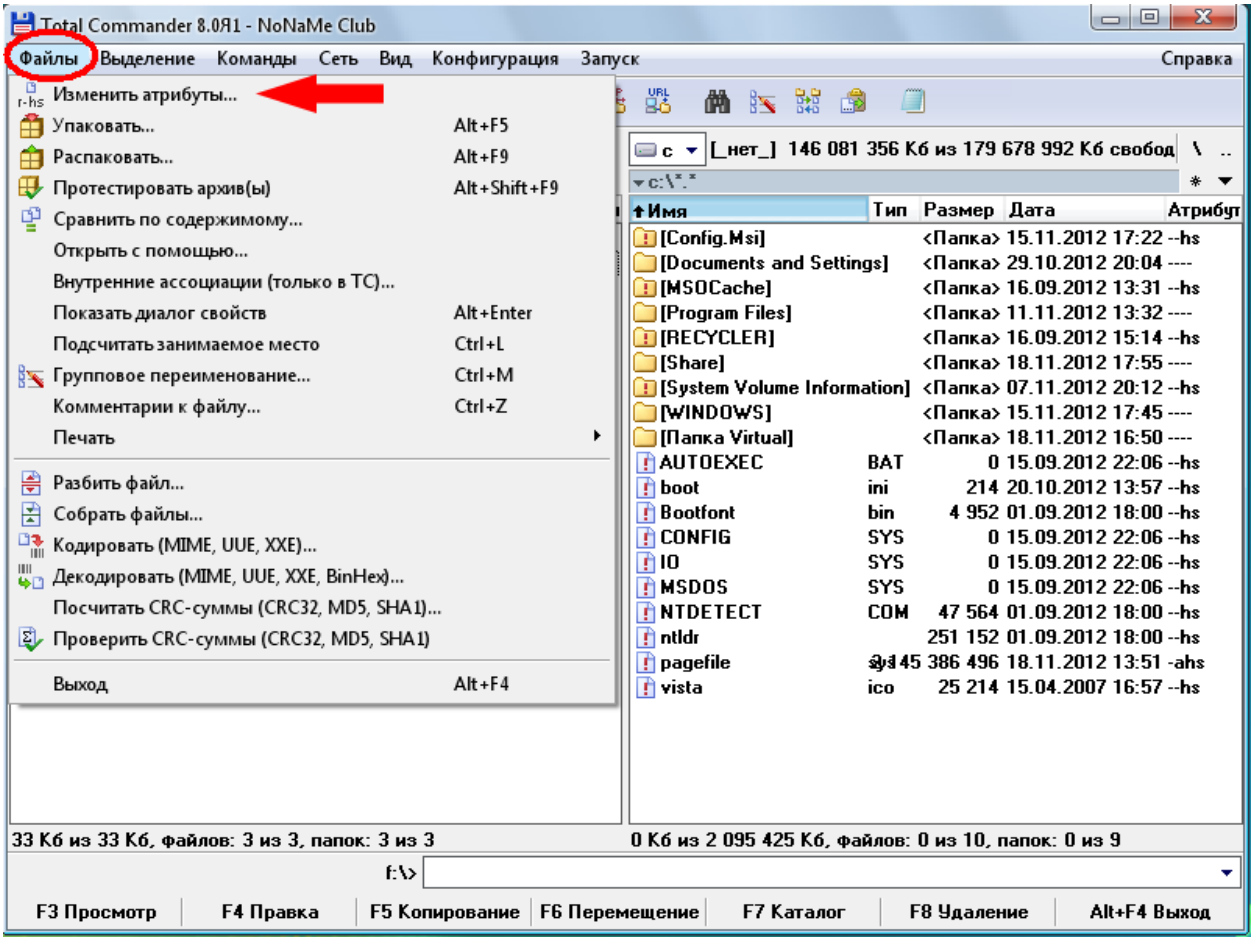
- В меню программы выбираем раздел Конфигурация - далее Настройка...



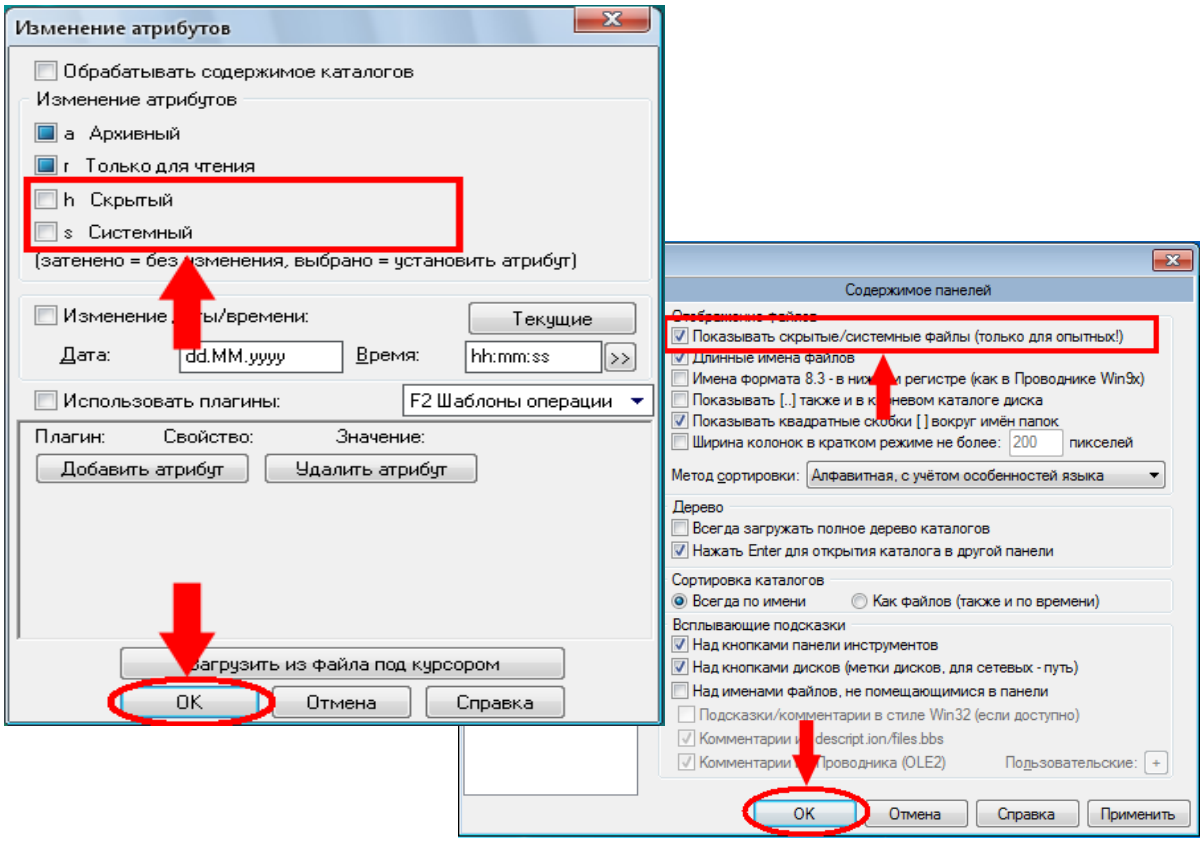
Б. Переходим в пункт Содержимое панелей - вставляем галку на Показать скрытые/системные файлы (только для опытных!) - сохраняем настройку ОК.

В. Выбираем свою флешку из списка дисков. В окне Total Commander видим восклицательные значки в папках и файлах. Это обозначает что эти папки и файлы скрыты. Выбираем папки (файлы) которые скрылись, удерживая кнопку CTRL и кликая мышкой на папки (файлы) или CTRL+A что бы выбрать всех папок и файлов.

Г. В меню программы выбираем Файл - Изменить атрибуты...



Д. В окне Изменение атрибутов кликаем на пункты "Скрытый" и "Системный" (пункты должны быть свободны) - нажимаем ОК.



3. Чтобы файлы не превращались в ярлыки , следует перед началом работы на usb-накопителе, проверить ПК на наличие вирусов.
Вставив накопитель в домашний ПК, так же проверить его на наличие вирусов.
В будущем стараться сохранять все файлы в стороннем источнике и убеждаться в том, что ПК на котором работаете безопасен.

Решение к задаче 3.5.

Существует несколько возможных решений нашей проблемы:

Первым и наиболее простым способом защиты от данного вида атак является внедрение в сервис такой системы взаимодействия с пользователем, когда для большинства действий совершаемых пользователем на странице, сайт запрашивает подтверждения и проверяет содержимое поля HTTP_REFERER по списку валидных вариантов. Но этот способ может быть небезопасен, и использовать его не рекомендуется.

Другим и более эффективным способом защиты является применение «секретного ключа», который хранится на сервере, и у клиента доступа к нему нет. Ключ представляет собой случайно сгенерированное значение и присваивается сессии пользователя. На основе этого ключа необходимо сгенерировать другое значение – «токен». Токен делается так, чтобы с одной стороны он был отличен от ключа, в частности, может быть много токенов для одного ключа, с другой – чтобы было легко проверить по токену, сгенерирован ли он на основе данного ключа или нет. Также для генерации токена

необходимо сгенерировать еще одно случайное значение – «соль». Таким образом формула токена выглядит следующим образом:

Токен = Соль + «:» + MD5(Соль + «:» + Секретный ключ),

где из неизвестных элементов остается только «:» - разделитель, и MD5 (англ. Message Digest 5) - 128-битный алгоритм шифрования.

Таким образом, мы получаем «случайное» значение, которое проверяется на сервере путем подстановки его составляющих. Далее, токен добавляется в качестве скрытого поля к каждой форме, генерируемой на сервере. И после, при отправке формы, сервер сначала проверит токен, и только в случае успешной проверки отошлет данные формы. В свою очередь злоумышленники элементарно не смогут сгенерировать валидную форму, так как не владеют «секретным ключом».

У данного решения есть свои варианты реализации. Первый вариант предполагает использование единственного токена для всех запросов пользователя. В таком случае, достаточно утечки токена в одном месте, как злоумышленник получает доступ к любому действию защищенному данным токеном. Второй вариант, более сложный, предполагает для каждого действия пользователя использовать свой токен, таким образом если была утечка одного токена, остальные действия пользователя остаются защищенными, так как защищены своими токенами. У данной варианта есть свои недостатки, к примеру, он более сложен в реализации и требователен к ресурсам. При выборе из этих двух вариаций, следует учесть, что на данный момент нет практических сведений о преимуществе варианта, где для каждого действия используется свой токен.

Решение к задаче 3.10

1. Чтобы решить первую проблему, необходимо загрузить список отозванных сертификатов и импортировать его в VIP NET CSP.

2. Проверить любые свойства сертификата (срок действия, информация о выданной организации и т.п.) можно с помощью панели управления Рутокен, открыть сертификат и перейти во вкладку «Свойства»

3. При установке носителя в новый компьютер необходимы драйвера (в данном случае Рутокен), скорее всего на данном компьютере они отсутствуют. А также сообщение «Установка заблокирована групповой политикой» может говорить о том, что USB порты отключены групповыми политиками предприятия, поэтому необходимо обратиться к системному администратору.

4. Перейди в Crypto Pro, проверить срок действия сертификата и закрытого контейнера ключа, очень часто срок действия контейнера заканчивается раньше, чем официальный срок действия сертификата. Если сертификат истек, то обратиться в удостоверяющий центр для получения новой ЭЦП.

5. Если сертификат действительный, проверить установлены ли корневые сертификаты удостоверяющего центра в Crypto Pro.

6. Попробовать подписать аттестат повторно, VIP NET CSP должен выдать сообщение что сертификат и пути сертификации действительны. Повторно загрузить файл аттестата на портал проверив что Правила пользования портала подписаны тем же лицом, которое подписывает аттестаты и приказ о назначении этого лица

ответственным загружен в личный кабинет. После подтверждения в личном кабинете обновить сведения о своём сертификате подписав и загрузив пробный файл. После этого загружать подписанный файл аттестата.

Решение к задаче 3.11

Идеального способа защиты программного обеспечения от несанкционированного использования и распространения не существует. Ни одна существующая система не обеспечит абсолютную защиту и не лишит потенциального взломщика самой возможности ее нейтрализации. Однако использование качественной и эффективной защиты может максимально усложнить процесс взлома программного продукта, более того, сделать взлом нецелесообразным с точки зрения потраченного на это времени и усилий.

С учетом проведенного анализа защищенности мультимедийных систем обучения, выявленных тенденций обеспечения информационной безопасности информационных ресурсов колледжа реализовали мультимедийную систему обучения, используя SQL-инъекции и защиты текста на страницах разделов (использование скрипта для запрета копирования**,** запрет выделения текста в CSS-стилях).

SQL-инъекции. SQL-инъекция представляет собой выполнение произвольного запроса к базе данных приложения с помощью поля формы или параметра URL. В случае использования стандартного языка Transact-SQL возможно вставить вредоносный код. В

результате чего будут получены, изменены или удалены данные таблиц. Чтобы предотвратить это, используйте параметризованные запросы, которые поддерживаются большинством языков веб-программирования.

Рассмотрим запрос:

```
SELECT * FROM table WHERE column = 'parameter';
```

Если злоумышленник изменит значение parameter на ' OR '1'='1, запрос примет следующий вид:

```
SELECT * FROM table WHERE column = '' OR '1'='1';
```

Так как '1' равен '1', атакующий получит доступ ко всем данным таблицы. Это позволит выполнить произвольный запрос, добавив в конец выражения SQL.

Уязвимость этого запроса легко устранить с помощью параметризации. Например, для приложения, написанного с использованием PHP и MySQLi, он выглядит так:

```php
$stmt = $pdo->prepare('SELECT * FROM table WHERE column = :value');
$stmt->execute(array('value' => $parameter));
```

Межсайтовый скриптинг (XSS) — тип атаки на веб-ресурсы, заключающийся во внедрении в страницу сайта вредоносного кода, который выполняется на компьютере пользователя, изменяет страницу и передаёт украденную информацию злоумышленнику.

Например, если на странице комментариев нет проверки входных данных, злоумышленник внедряет вредоносный код JavaScript. В результате у пользователей, которые просматривают комментарий, выполняется код, и данные об авторизации из cookies-файлов отправляются атакующему.

Особенно подвержены этому виду атаки современные веб-приложения, где страницы построены из пользовательского контента, интерпретируемого фронтенд-фреймворками вроде Angular и Ember. В эти фреймворки встроена защита от межсайтового скриптинга, но смешанное формирование контента на стороне сервера и клиента создает новые комплексные атаки: внедрение директив Angular или хелперов Ember.

При проверке сосредоточьтесь на пользовательском контенте, чтобы избежать некорректной интерпретации браузером. Это похоже на защиту от SQL-инъекций. При динамической генерации HTML-кода используйте специальные функции для изменения и получения значений атрибутов.

Например, element.setAttribute и element.textContent), а также шаблонизаторы, которые выполняют экранизацию специальных символов автоматически.

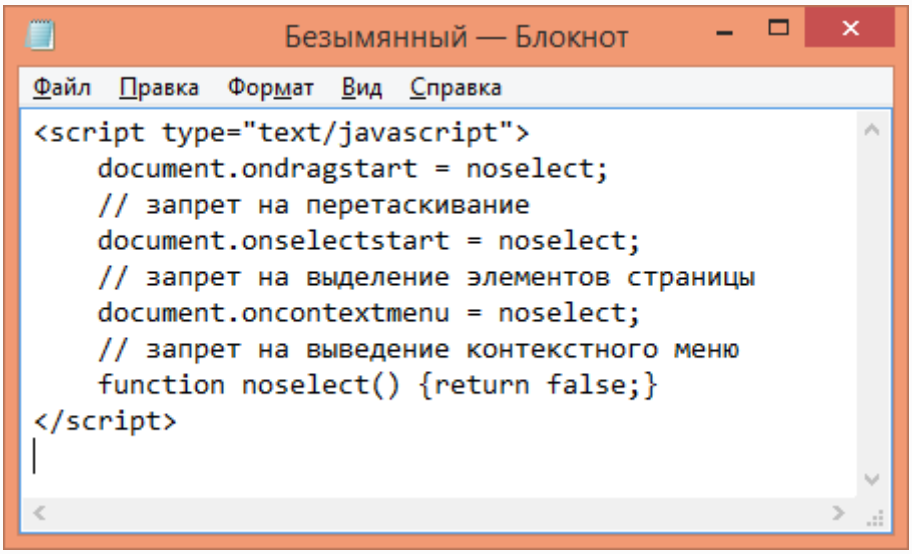
Политика безопасности содержимого (CSP) — ещё один инструмент защиты от XSS-атак. CSP — заголовки сервера, определяющие белый список источников, откуда разрешена загрузка данных для разных типов ресурсов. Например, запрет запуска скриптов со стороннего домена или отключение функции eval(). Благодаря политикам CSP даже при внедрении вредоносного кода в страницу его выполнение становится невозможным.

Следующая мера информационной защиты мультимедийной системы обучения по дисциплине «Технические средства информатизации» - защита текста на главной странице или на страницах разделов.

Контент на этих страницах копируют, в основном, вручную. Поэтому, здесь применимы следующие методы.

1. *Использование скрипта для запрета копирования***.** На странице можно добавить скрипт, который не позволит пользователю вручную выделить и скопировать текст.

Пример скрипта приведен на скриншоте ниже.



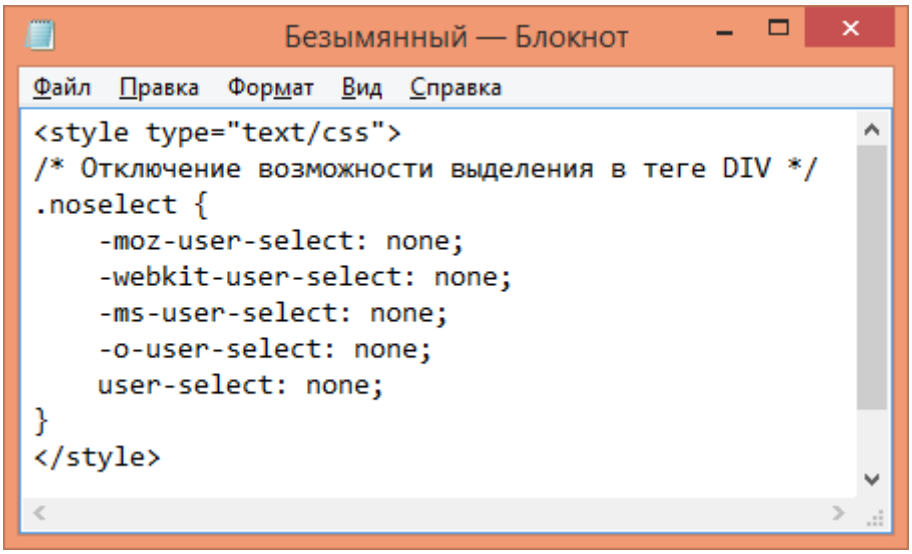
Приведенный выше скрипт запрещает выделение части текста, а также отключает контекстное меню во всем документе, если злоумышленник захочет открыть код страницы.

Минус данного способа в том, что пользователи иногда переходят по ссылкам, кликая правой клавишей мыши. Подобными скриптами можно создать ряд неудобств и понизить количество просмотров страниц своего сайта, и соответственно, конверсию в целевые действия.

Этот метод легко обойти, открыв источник страницы через главное меню браузера, либо отключив в браузере скрипты и копируя необходимое без всяких запретов. Однако, вероятность воровства текста неопытным «копирайтером» существенно снизится.

2. *Запрет выделения текста в CSS-стилях.* Аналогичный предыдущему методу, но можно уже не использовать скрипт, а прописать отдельный стиль (например, класс «noselect»), в котором запрещается выделять текст.

Пример кода приведен на скриншоте ниже.



Этот метод имеет уже немного меньше недостатков: с помощью отключения скриптов возможности выделения текста все равно не будет, а отключить стили в браузере сложнее, однако, этот метод все также легко обойти, если открыть HTML-код страницы.

Распределяйте права доступа к файлам

Разрешения файла (file permissions) определяют КТО и ЧТО может с ним делать.

В *nix системах у файлов 3 варианта доступа, которые представляются в виде цифр:

- «Read» (4) — чтение содержимого файла;
- «Write» (2) — изменение содержимого файла;
- «Execute» (1) — выполнение программы или скрипта.

Чтобы установить множественные разрешения, достаточно сложить их числовые значения:

- «Чтение» (4) + «запись» (2) = 6;
- «Чтение» (4) + «запись» (2) + «выполнение» (1) = 7.

При распределении прав пользователи делятся на 3 типа:

1) «Owner» (владелец) — создатель файла (изменяем, но может быть только один);

2) «Group» (группа) — группа пользователей, которые получают разрешения;

3) «Others» (прочие) — остальные пользователи.

Установка владельцу прав доступа на чтение и запись, группе — на чтение, прочим — запрет доступа выглядит так:

	Чтение	Запись	Выполнение
Владелец	2	4	0
Группа	0	4	0
Прочие	0	0	0

Итоговое представление: `640`.

Для каталогов аналогично, но флаг «выполнить» значит сделать рабочей директорией. При установке CMS-разрешения, как правило, устанавливаются корректно с точки зрения безопасности. Однако в Интернете часто советуют решать проблемы прав доступа установкой на все файлы значения `666` или `777`. Этот совет помогает решить проблему, но открывает серьёзную уязвимость, потому что всем появляется право изменить (вставить вредоносный код) или удалить файлы на сервере.

Распределяйте права доступа к файлам на сервере в соответствии с задачами пользователей.

Внедрение вышеописанных мер привело к повышению уровня информационной безопасности при использовании мультимедийно системы обучения в ГБПОУ «Южно-Уральский государственный колледж».

Основным показателем обеспечения безопасности мультимедийной системы обучения является повторный анализ количества обращений к исполняемому файлу запуска программы.

Разработанные и внедренные рекомендации, а именно: настройка политики безопасности сайта, распределение прав доступа к файлам, применение SQL-инъекции совместно с использованием скрипта для запрета копирования и запрет выделения текста в CSS-стилях, позволили сократить данный показатель к абсолютному минимуму, так как у обучающихся заблокирован доступ не только к исходному файлу, а также к файловой системе компьютера в целом.

Доступ к исполняемому файлу запуска мультимедийной системы обучения остался открытым для студентов, но при этом из общего доступа были убраны исходные файлы проекта. Повторный анализ выявил 12 обращений к исполняемому файлу запуска МСО.

Внедрение программы удалённого доступа позволило преподавателям более эффективно осуществлять контроль за деятельностью обучающихся как во время тестирования, так и во время выполнения заданий.

Результаты бета-тестирования, разработанной мультимедийной системы обучения по дисциплине «Технические средства

информатизации» оцениваем положительно и считаем доказанной гипотезу исследования.

Таким образом, можно выделить следующие меры информационной защиты мультимедийной системы обучения:

1. Настройка политики безопасности сайта.
2. Распределение прав доступа к файлам.
3. SQL-инъекции.
4. Защита текста на главной странице или на страницах разделов (использование скрипта для запрета копирования, запрет выделения текста в CSS-стилях).

Решение к задаче 3.12

1. Исходя из топологии сети выясняем, что все ПК конструкторского отдела связанны между собой локальной сетью. В первую очередь при вирусном заражении нам необходимо локализовать его, для этого связываемся с отделом информационных технологий и отключаем данный сегмент локальной сети. Дополнительно согласовываем с начальником отдела прекращение работы с машинными носителями информации, которые могли быть заражены.

2. После того, как воздействие вирусов локализовано в рамках одного отдела, приступаем к проверке ПК сотрудников конструкторского отдела. Для этого сотрудник отдела информационной безопасности записывает необходимые утилиты и иные программные средства защиты информации на оптический диск, с целью не заразить машинный носитель информации.

3. Во время проверки ПК отдела выясняется, что заражение выявлено только на одном из них, сотрудник которого и сообщил в подразделение безопасности. Оценив загруженность жёсткого диска заражённого ПК и наличие процессов, начатых сторонней вирусной программой принимается решение о перезагрузке данного ПК и физическом отключении его от кабеля локальной сети. До загрузки операционной системы включается антивирусная проверка, ставим в антивирусе галочку, что добавлять заражённые файлы в карантин, а не удалять.

4. Проводим проверки всех потенциально заражённых носителей информации в отделе. Берём объяснение с сотрудника, на чьём ПК был обнаружен вирус первоначально

5. В объяснении сотрудник пишет, что сегодня с утра, перед проходной на завод он нашёл флешку на 64 Гб и захотел её взять. В перерыв он решил посмотреть, что содержится на этой флешке и спустя некоторое время ПК стал ощутимо тормозить. Также сотрудник передал данную флешку представителю отдела информационной безопасности.

6. После лечения заражённого ПК с помощью антивирусных средств выявлено, что часть конструкторской документации была зашифрована и не представляется возможным работать с ней. Но так как ежеквартально во всех отделах предприятия проводится резервное копирование, данные файлы были найдены и после лечения ПК перенесены на жёсткий диск для дальнейшей работы.

Выводы: Данный инцидент информационной безопасности стал возможен потому что не соблюдались правила антивирусной

защиты(проверка всех носителей информации перед началом работы с ними) и правила использования носителей информации (был подключен машинный носитель информации, не учтённый на предприятии, а также содержимое которого неизвестно). Так как на этом носителе информации был обнаружен компьютерный вирус, необходимо провести внутреннее расследование и по возможности уточнить с помощью камер видеонаблюдения, кем была оставлена данная флешка, для учёта в дальнейшем.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Стандарты

ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования .

ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические ___ . Госстандарт России. - М., 1995.

ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. - М., 2006.

ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие требования. Госстандарт России. - М., 2006.

ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем». – М.: Стандартинформ, 2015.

Учебные издания, научные публикации.

1. Абрамов О.Ю. Диверсионный анализ Технических Систем на переходном этапе развития - [Электронный ресурс] // URL: http://triz-summit.ru/file.php/id/f5015/nme/TRIZ- (дата обращения: 15.02.2023)

2. Буслов Д.И., Холкин И.Н. Как, используя диверсионный анализ ТРИЗ, найти критическую уязвимость, грозящую безопасности SP Hn // Математика и информационные технологии в нефтегазовом комплексе. 2015. №2. URL: http://cyberlenink.ru/rticle/n/kk-ispolzuy-diversionnyy-nliz-triz-nyti-kriticheskuyu-uyzvimost-grozyschuyu-bezopsnosti-sp-hn (дата обращения: 11.04.2023).

3. Галатенко В.А. Идентификация и аутентификация, управление доступом [Электронный ресурс]: http://citforum.ru/security/articles/galatenko/- (дата обращения - 01.03.2023)

4. Гафарова Е.А. Задачный подход в решении проблемы формирования творческих умений старшеклассников при изучении компьютерных информационных технологий. // Известия Российского государственного педагогического университета им. А.И. Герцена. 2006. Т. 5. № 23. С. 116-119.

5. Гафарова Е.А. Организационно-правовое обеспечение информационной безопасности. // Учебное пособие, ЮУрГГПУ, Челябинск, 2019

6. Гафарова Е.А. Программно-аппаратные средства обеспечения информационной безопасности. Практикум. Челябинск, 2021.

7. Гафарова Е.А., Синицын Ф.В. К вопросу проектирования онтологий предметной области при подготовке магистров по направлению информационная безопасность.// Инновационные технологии в подготовке современных профессиональных кадров: Опыт, проблемы. Сборник научных трудов. 2016, Челябинский филиал РАНХиГС, 56-59 с.

8. Грицай Л.А. Информационная война в социальных сетях как угроза национальной безопасности России // Современные научные исследования и инновации. 2014. № 10 – [Электронный ресурс] – URL: http://web.snuk.ru/issues/2014/10/38607 (Дата обращения: 04.05.2023).

9. Диденко Е.В., Гафарова Е.А., Диденко Г.А. Педагогические условия формирования готовности обучающихся колледжа к противодействию вовлечению в киберэкстремистскую деятельность.//Современные наукоемкие технологии. 2019. № 3-2, с. 280-283.

10. Кармановский Н.С., Михайличенко О.В., Савков С.В. Организационно-правовое и методическое обеспечение информационной безопасности: Учебное пособие. - СПб.: НИУ ИТМО, 2013. - 148 с.

11. Коноваленко С. А., Королев И. Д. Выявление уязвимостей информационных систем. // Инновации в науке: сб. ст. по матер. LXI

междунар. науч.-практ. конф. № 9(58). – Новосибирск: СибАК, 2016. – С. 12-20.

12. Мезенов А.С., Гафарова Е.А. О реализации конституционного права граждан на доступ к информации в условиях интенсификации сетевого взаимодействия.//Сборник научных трудов конференции «Инновационные технологии в подготовке современных профессиональных кадров: опыт, проблемы», 2016, Издательство: Челябинский филиал РАНХиГС, с.94-99

13. Salamatov A., Gafarova E., Belevitin V., Gordeeva D., Gafarov M. MACHINE LEARNING METHODS AND QUALIMETRIC APPROACH TO DETERMINE THE CONDITIONS FOR TRAIN STUDENTS IN THE FIELD OF ENVIRONMENTAL AND ECONOMIC ACTIVITIES. // International Journal of Emerging Technologies in Learning. 2021. Т. 16. № 3. С. 72-85.

Учебное пособие

Елена Аркадьевна Гафарова

СБОРНИК КЕЙС-ЗАДАЧ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Издательство «Библиотека А.Миллера»
454080, г. Челябинск, ул. Свободы, 159
6.7 усл.- печ. л.