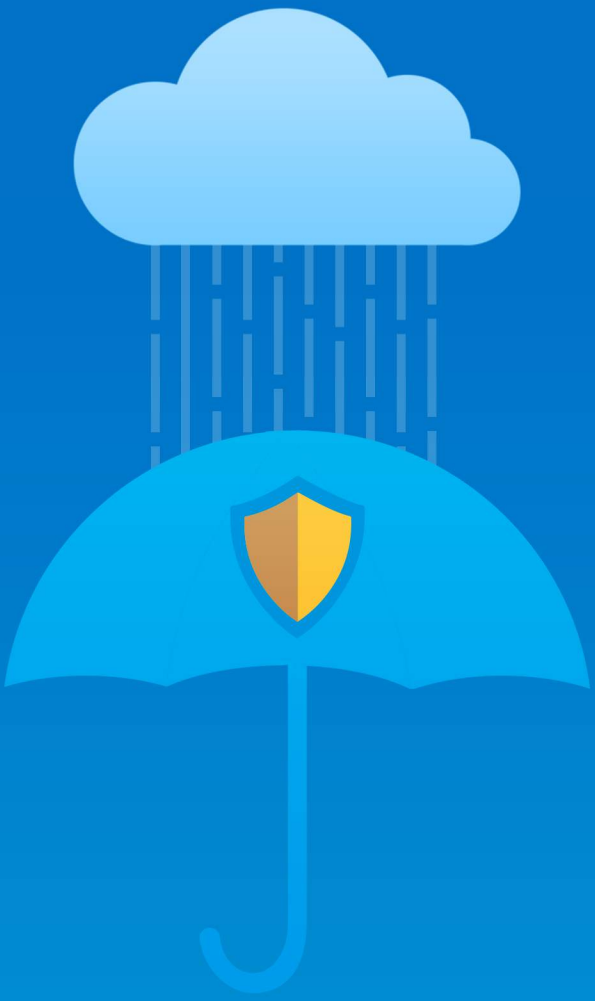


Survival Guide

Правила кибергигиены

1. Не использовать нелицензионное ПО.

Использование нелицензионного программного обеспечения является одной из самых распространенных причин успешных атак на информационные системы и их пользователей. Под информационной системой в данном случае может пониматься как инфраструктура большой компании, так и простая домашняя локальная сеть. Причины, по которым использование нелицензионного ПО может привести к плачевным последствиям, следующие:

Отсутствие своевременных обновлений.
Зачастую хакеры, осуществляющие разработку активаторов, таблеток, crack'ов, средств удаленной активации, не включают в свои «продукты» возможность осуществления своевременных обновлений операционной системы. Это означает, что если будет обнаружена какая-то уязвимость и производитель системы выпустит срочное обновление, те пользователи, которые используют нелицензионное ПО не будут иметь возможности эти обновления получить. А следовательно еще долгое время их компьютеры будут подвержены опасности. Использование лицензионного ПО, в свою очередь, подразумевает, что пользователь сразу же получает возможность установки всех выходящих патчей.

Закладки от лиц, осуществивших взлом системы.
Хакеры, осуществляющие разработку специфического ПО для активации систем, делают это не из благородных соображений. В такого рода программных средствах регулярно находятся так называемые "закладки". Закладка – это программный код, который может осуществлять достаточно широкий спектр действий: от сбора информации, до бомбы замедленного действия, когда ничего не подозревающий пользователь в определенный момент времени может потерять управление своим компьютером.

Отсутствие технической поддержки.
Техническая поддержка бывает крайне важна, когда пользователь сталкивается с каким-либо непредвиденным поведением системы, либо просто не может самостоятельно разобраться с какими-либо настройками. Грамотная поддержка поможет решить проблему максимально безопасным образом. Отсутствие поддержки – серьезный недостаток с точки зрения безопасности.

2. Пользоваться антивирусными средствами, а также осуществлять своевременное и регулярное обновление баз сигнатур вирусов.

Ни для кого не секрет, что антивирусное программное обеспечение хоть и не является панацеей от всех угроз, но представляет собой первую линию обороны любой информационной системы. Как только появляется новый вирус, вирусные аналитики начинают исследовать его поведение и пополняют базу сигнатур. При попадании изученного вируса на пользовательский ПК, антивирусное средство моментально реагирует на это событие и предупреждает пользователя о потенциальной угрозе. Важно, чтобы базы сигнатур своевременно обновлялись и антивирусное ПО было сконфигурировано таким образом, чтобы предоставить оптимальную защиту пользователю.

3. Не устанавливать никакие программные средства из недоверенных источников.

Данная рекомендация предполагает, что пользователь полностью осознает, какую угрозу могут нести в себе бесплатные программные средства, особенно в том случае, если загрузка осуществляется с непроверенных сайтов или съемных носителей. Если же такая необходимость есть, пользователь должен понимать, что сам несет ответственность за все связанные с использованием такого ПО риски.

4. Осуществлять своевременное обновление как операционной системы, так и всего остального используемого программного обеспечения.

Как уже было сказано выше в п.1.1, своевременное обновление ПО является необходимым действием по обеспечению безопасной и бесперебойной работы информационной системы. Это касается не только операционной системы, но и всего используемого прикладного программного обеспечения, драйверов и многого другого. Выпускаемые патчи призваны максимально обезопасить пользователей, поэтому категорически не рекомендуется пренебрегать своевременными и регулярными обновлениями.

5. Соблюдать правила кибергигиены в областях:
- использования съемных носителей
- пользовательской грамотности (переход по ссылкам, открытие вложений и т.д.)
- защиты от социальной инженерии
- использования правильной парольной политики

6. Постараться закрывать неиспользуемые порты, отключать неиспользуемые службы, а также просто минимизировать количество запущенных программных средств в случае, если в них нет необходимости.

Например, уязвимость Ethernalblue позволяла вирусам распространяться столь стремительно ввиду того, что по умолчанию был открыт 445 порт. Чем больше программного обеспечения используется на каждой конкретной машине, тем больше риск, что в одном из программных средств будет найдена уязвимость и пользователь подвергнется риску.

7. Не подключаться к непроверенным сетям Wi-Fi.

Злоумышленники могут использовать специальным образом организованную точку доступа для сбора информации о жертве путем проведения атаки Man-in-the-Middle (человек посередине). Это позволит злоумышленникам перехватывать и подменять пакеты данных, передаваемых по этой сети, что может привести к компрометации или краже данных пользователя.

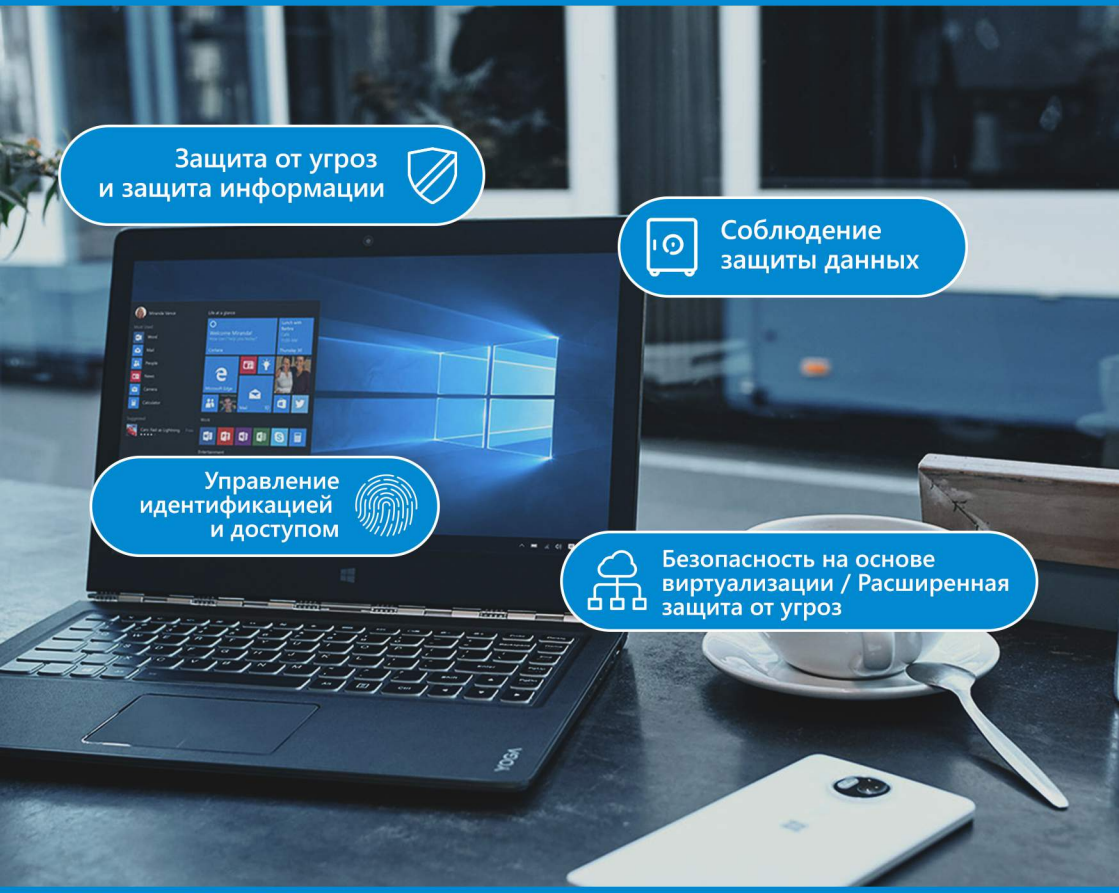
8. Регулярно проводить проверку безопасности конфигурации информационной системы.

Данная рекомендация предполагает, что пользователь проявляет достаточную бдительность при пользовании информационной системой и сможет вовремя реагировать на появляющиеся угрозы и учитывать их при организации своей информационной системы. Все приведенные выше рекомендации ориентированы на любого пользователя ПК.
Если же речь идет о крупной промышленной информационной системе, либо ИС организации, то требования становятся шире. Первое, на что стоит обратить внимание в этом случае - это соблюдение требований международного стандарта ISO-27001. Этот стандарт предписывает, каким образом должен быть организован процесс информационной безопасности в организации. Важными его пунктами, помимо упомянутых

выше, являются также соблюдение требований своевременного оповещения персонала о существующих угрозах и принятых в организации правилах защиты от них. К сожалению, человек по-прежнему остается самым уязвимым звеном в процессе обеспечения информационной безопасности любой системы, поэтому проведение своевременных ознакомительных работ играет ключевую роль в обеспечении ИБ организации. Кроме того, стандарт ISO-27001 предписывает, каким образом регламентируется процесс ИБ с точки зрения правил и политик организации, что позволяет успешно интегрировать процедуры ИБ в функционирование данной организации.

Survival Guide

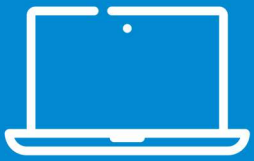
Бизнес строится на **ДОВЕРИИ**
ДОВЕРИЕ строится на **Подлинности**



Безопасность предприятия без ущерба для Производительности

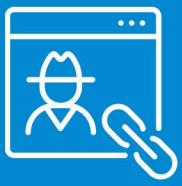
Целостное и инновационное решение для защиты пользователей, устройств, приложений и данных

Управление идентификацией и доступом



Управление мобильными устройствами и приложениями

Защита информации



Защита от угроз

- Защита на входе
- Защита ваших данных повсеместно
- Обнаружение и устранение атак

Поддержка клиентов для создания прочной основы.

Позаботьтесь о своей защите, если...

Цена программного обеспечения слишком хороша, чтобы быть правдой

Программное обеспечение приходит из приложений для обмена файлами или распространяется через электронную почту, социальные сети или веб-сайты

Ключи продуктов продаются отдельно от программного обеспечения или поставляются в комплекте с несколькими ключами продуктов

Упаковка была открыта или не является стандартной упаковкой Microsoft

Ключ продукта или код установки не работает, или программное обеспечение не может быть активировано

Программное обеспечение поставляется в нестандартной или непрофессиональной упаковке

Клиентов просят загрузить файлы для завершения активации

ПК или другое устройство поставляется с уже активированным программным обеспечением

Решения Партнера в области безопасности облачных сервисов

Windows and Windows Server

Windows 10 и Windows Server включают в себя ведущие в отрасли технологии шифрования, защиты от вредоносных программ и решения для идентификации и доступа, которые позволяют переходить от паролей к более безопасным формам аутентификации:

- **Windows Hello** - это удобная альтернатива паролей корпоративного уровня, использующая естественный (биометрический) или знакомый (ПИН) метод проверки личности, который обеспечивает преимущества безопасности смарт-карт без необходимости использования дополнительных периферийных устройств.

- **Windows Защитник** - это надежное решение для защиты от вредоносных программ, которое готово работать сразу после установки. Windows Защитник способен быстро обнаружить и защитить ваши устройства от новых вредоносных программ в любой части вашей информационной среды.

- **Device Guard** позволяет заблокировать ваши устройства и серверы для защиты от новых и неизвестных вариантов вредоносных программ и продвинутых постоянных угроз. В отличие от основанных на обнаружении решений, таких как антивирусные программы, которые требуют постоянного обновления для обнаружения последних угроз, Device Guard блокирует устройства, чтобы они могли запускать только авторизованные приложения, которые вы выбрали, что является эффективным способом борьбы с вредоносными программами.

- **Credential Guard** - это функция, которая изолирует ваши секреты на устройстве, например, токены единого входа, от доступа даже в случае полного взлома операционной системы Windows. Это решение принципиально предотвращает использование атак, от которых трудно защититься, таких как «передача хэша».

- **Шифрование диска BitLocker** в Windows 10 и Windows Server обеспечивает корпоративное шифрование, которое помогает защитить ваши данные в случае потери или кражи устройства. BitLocker полностью шифрует диски и флэш-диски вашего компьютера, чтобы предотвратить доступ к вашим данным неавторизованным пользователям.

- **Windows Information Protection** определяет, где прекращается BitLocker. Хотя BitLocker защищает весь диск устройства, Windows Information Protection защищает ваши данные от неавторизованных пользователей и приложений, работающих на компьютере. Это также помогает предотвратить утечку данных из деловых в некоммерческие документы или в Интернет.

- **Windows Defender Advanced Threat Protection (ATP)** определяет, где прекращается BitLocker. Хотя BitLocker защищает весь диск устройства, Windows Information Protection защищает ваши данные от неавторизованныхпользователей и приложений, работающих на компьютере. Это также помогает предотвратить утечку данных из деловых в некоммерческие документы или в Интернет.

- **Экранированные виртуальные машины** позволяют использовать BitLocker для шифрования дисков и виртуальных машин (ВМ), работающих на Hyper-V, для предотвращения атак скомпрометированных и злонамеренных администраторов на содержимое защищенных ВМ.

- **Расширенная защита от угроз (ATP)** Защитника Windows позволяет вашим операционным группам безопасности обнаруживать, расследовать, локализовать и реагировать на нарушения данных в вашей сети. С помощью Защитника Windows ATP вы получаете расширенные возможности обнаружения, расследования и реагирования на нарушения на всех ваших конечных точках, сохраняя до 6 месяцев исторических данных, даже когда конечные точки находятся в автономном режиме, за пределами сетевого домена, перезаписаны или больше не существуют. Защитник Windows ATP помогает выполнить ключевое требование GDPR, которое предусматривает четкие процедуры для обнаружения, расследования и сообщения о нарушениях данных.

Office 365

Office 365 обладает несколькими возможностями, которые помогают выявлять угрозы и реагировать на них:

- **Функция предотвращения потери данных (DLP) в Office и Office 365** позволяет идентифицировать более 80 распространенных конфиденциальных типов данных, включая финансовую, медицинскую и личную информацию.

- **Поиск контента в Центре безопасности и соответствия требованиям Office 365** позволяет выполнять поиск по почтовым ящикам, общим папкам, группам Office 365, командам Microsoft, сайтам SharePoint Online, местоположениям One Drive for Business и Skype для бизнеса.

- **Поиск eDiscovery в Office 365** можно использовать для поиска текста и метаданных в содержимом ваших активов Office 365 - SharePoint Online, OneDrive для бизнеса, Skype для бизнеса Online и Exchange Online.

- **Office 365 Advanced eDiscovery**, основанный на технологиях машинного обучения, может помочь вам быстро и с большей точностью идентифицировать документы, относящиеся к определенному предмету (например, расследование соответствия), чем при традиционном поиске по ключевым словам или ручном просмотре огромного количества документов. Расширенное обнаружение электронных данных может значительно снизить затраты и усилия по выявлению соответствующих документов и взаимосвязей данных, используя машинное обучение, чтобы обучить систему интеллектуальному исследованию больших наборов данных и быстро сосредоточиться на том, что важно, - сократить объем данных перед проверкой.

- **Расширенное управление данными** использует интеллектуальные и машинные знания, чтобы помочь вам находить, классифицировать, устанавливать политики и предпринимать действия для управления жизненным циклом данных, которыенаиболее важны для вашей организации.

- **Расширенная защита от угроз (ATP) для Exchange Online** помогает защитить вашу электронную почту от новых, сложных атакредоносных программ в режиме реального времени. Он также позволяет создавать политики, которые помогают предотвратить доступ пользователей к вредоносным вложениям или вредоносным веб-сайтам, связанным по электронной почте. ATP для Exchange Online включает в себя защиту от неизвестных вредоносных программ и вирусов, защиту от вредоносных URL-адресов, а также расширенные возможности создания отчетов и отслеживания URL-адресов.

- **Управление правами на доступ к данным (IRM)** помогает вам и вашим пользователям предотвращать печать, пересылку, сохранение, редактирование или копирование конфиденциальной информации посторонними лицами. С помощью IRM в SharePoint Online вы можете ограничить действия, которые пользователи могут выполнять над файлами,

загруженными из списков или библиотек, например, распечатывать копии файлов или копировать из них текст. IRM в Exchange Online позволяет предотвратить утечку конфиденциальной информации в сообщениях электронной почты и вложениях по электронной почте, в Интернете и в автономном режиме.

- **Управление мобильными устройствами (MDM) для Office 365** позволяет настраивать политики и правила, помогающие защищать зарегистрированных пользователей iPhone, iPad, устройства Android и телефоны Windows и управлять ими. Например, вы можете удаленно стереть устройство и просматривать подробные отчеты об устройстве. Office 365 также использует многофакторную аутентификацию, чтобы обеспечить дополнительную безопасность.

Enterprise Mobility + Security (EMS) Suite

EMS предоставляет технологии, которые помогают вам обнаруживать, контролировать и защищать личные данные, хранящиеся в вашей организации, а также выявлять потенциальные «слепые зоны» и выявлять случаи нарушения данных.

- **Microsoft Intune** предоставляет возможности управления мобильными устройствами, мобильными приложениями и ПК с помощью облака. Используя Intune, вы можете предоставить своим сотрудникам доступ к корпоративным приложениям, данным и ресурсам практически из любого места практически на любом устройстве, одновременно обеспечивая высокую безопасность корпоративной информации.

- **Microsoft Advanced Threat Analytics (ATA)** - это локальный продукт, помогающий специалистам по ИТ-безопасности защитить свою организацию отрасширенных целевых атак путем автоматического анализа, изучения и выявления нормального и ненормального поведения объекта (пользователя, устройств и ресурсов). ATA выявляет расширенные постоянные угрозы (APT) локально, обнаруживая подозрительное поведение пользователей и объектов (устройства и ресурсы), используя машинное обучение и информацию в локальных Active Directory, системах SIEM и журналах событий Windows. Он также обнаруживает известные вредоносные атаки (например, Pass the Hash). Наконец, он предоставляет простой график атаки с четкой и актуальной информацией об атаке, поэтому вы можете быстро сосредоточиться на том, что важно.

- **Azure Active Directory (Azure AD) Premium** обеспечивает обнаружение угроз на уровне личности в облаке. Azure AD отслеживает использование приложений и защищает ваш бизнес от расширенных угроз с помощью отчетов и мониторинга безопасности. Отчеты о доступе и использовании обеспечивают видимость целостности и безопасности каталога вашей организации. Кроме того, Azure AD обеспечивает защиту личных данных с помощью уведомлений, анализа и рекомендуемых исправлений.

- **Microsoft Cloud App Security** - это комплексный сервис, который обеспечивает более глубокую наглядность, комплексный контроль и улучшенную защиту ваших данных в облачных приложениях. Вы можете видеть, какие облачные приложения используются в вашей сети — идентифицировать более 13 000 приложений со всех устройств - и получать оценки рисков и текущую аналитику.

- **Microsoft Azure Information Protection** поможет определить, какие у вас конфиденциальные данные и где они находятся. Вы можете либо запросить данные, помеченные с определенной чувствительностью, либо разумно идентифицировать конфиденциальные данные при создании файла или электронного письма. После идентификации вы можете автоматически классифицировать и маркировать данные - все в соответствии с желаемой политикой компании.

Облачные службы Microsoft

Как подробно описано в Центре доверия Microsoft, Облачные службы Microsoft принимают решительные меры для защиты данных клиентов от несанкционированного доступа или использования посторонними лицами.

- **Azure Active Directory** - это решение для управления учетными записями и доступом в облаке. Он управляет удостоверениями и контролирует доступ к Azure, локальным и другим облачным ресурсам, данным и приложениям. С помощью Azure Active Directory Privileged Identity Management вы можете назначить временные административные права Just-In-Time (JIT) соответствующим пользователям для управления ресурсами Azure.

- **Центр безопасности Azure** предоставляет вам возможность контроля и безопасности ваших ресурсов Azure. Он постоянно отслеживает ваши ресурсы и предоставляет полезные рекомендации по безопасности. Он позволяет вам определять политики для ваших подписок Azure и групп

ресурсов на основе требований безопасности вашей компании, типов приложений, которые вы используете, и чувствительности ваших данных. Он также использует рекомендации по безопасности на основе политик, чтобы помочь владельцам сервисов реализовать необходимые элементы управления, например, включить защиту от вредоносных программ или дисков для ваших ресурсов. Центр безопасности также помогает вам быстро развертывать службы безопасности и устройства от Microsoft и партнеров для усиления защиты вашей облачной среды.

- **Шифрование данных в Azure** обеспечивает безопасность ваших данных в покое и в пути. Например, вы можете автоматически зашифровывать свои данные, когда они записываются в хранилище Azure с использованием шифрования службы хранилища. Кроме того, вы можете использовать Azure Disk Encryption для шифрования операционных систем и дисков с данными, используемых виртуальными машинами Windows и Linux. Данные защищаются при передаче между приложением и Azure, поэтому они всегда остаются в высшей степени безопасными.

- **Хранилище ключей Azure** позволяет защитить ваши криптографические ключи, сертификаты и пароли, которые используются для защиты ваших данных. Хранилище ключей использует аппаратные модули безопасности (HSM) и разработано таким образом, чтобы вы могли контролировать свои ключи и, следовательно, свои данные, в том числе гарантировать, что Microsoft не сможет увидеть или извлечь ваши ключи. Вы можете отслеживать и проверять использование сохраненных ключей с помощью ведения журнала Azure и импортировать свои журналы в Azure HDInsight или в свою систему защиты информации и управления событиями (SIEM) для дополнительного анализа и обнаружения угроз.

- **Microsoft Antimalware** для облачных служб и виртуальных машин Azure — это бесплатная функция защиты в режиме реального времени, которая помогает вам выявлять и удалять вирусы, шпионское ПО и другое вредоносное ПО, предназначенное для кражи данных, с настраиваемыми оповещениями, которые сообщают вам об известных вредоносных или нежелательных программах, пытающихся установить себя или запустить в ваших системах Azure.

GDPR: не только для Европы

Общие нормы защиты данных (GDPR) — устанавливает новый стандарт в отношении конфиденциальности, безопасности и соответствия нормативным требованиям. GDPR предъявляет новые требования в следующих областях:

- Более полный контроль физических лиц над персональными данными
- Гарантированная прозрачность использования данных
- Использование механизмов безопасности и контроля для защиты данных

GDPR открывает существенные рыночные возможности для поставщиков систем безопасности и хранения. Недавно проведенное исследование показывает, что 75 % компаний из США, называющих GDPR своим приоритетом, заложили в бюджет не менее 1 млн долларов США на соблюдение соответствующих требований. Еще одно исследование показывает, что в Европе эта цифра варьируется от 100 000 до нескольких миллионов евро в зависимости от текущего положения дел в организации.

Сфера применения GDPR гораздо шире, чем кажется многим. Этот закон вводит новые правила для компаний, государственных органов, некоммерческих организаций и прочих инстанций, предлагающих товары и услуги на территории Европейского союза (ЕС) или собирающих и анализирующих данные, связанные с резидентами ЕС, независимо от местоположения последних. Нормы GDPR применимы к организациям любых масштабов, работающим в любых отраслях.

Вывод: нормы GDPR могут применяться и к вашему бизнесу, и к бизнесу ваших клиентов. Для начала нужно понять, какими данными вы владеете и где они хранятся. Нормы GDPR регулируют сбор, хранение, использование и предоставление «персональных данных». В контексте GDPR термин «персональные данные» трактуется очень широко: это любые данные, имеющие отношение к физическому лицу, которое было идентифицировано или которое можно идентифицировать. Данные могут храниться в:

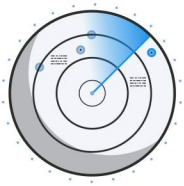
- базах данных клиента
- формах обратной связи, заполняемых клиентами
- содержимом электронной почты
- фотографиях
- видеозаписях с камер наблюдения
- записях программ лояльности
- кадровых базах данных

О нас

«Центр анализа и расследования кибер атак» (сокр. ЦАРКА) – одна из ведущих центрально-азиатских организаций в области информационной безопасности. Центр образован в 2015 г. и за время своего существования завоевал признание специалистов в области информационной безопасности не только стран СНГ, но и за рубежом.

ЦАРКА представляет широкий спектр услуг в области оценки защищенности, в том числе проведение аудитов информационной безопасности, тестов на проникновение, подготовку и сертификацию согласно стандартам в области информационной безопасности, анализ защищенности банковских систем, веб-приложений, бизнес приложений, информационных инфраструктур.

Наши услуги

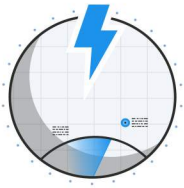


Аудит информационных систем

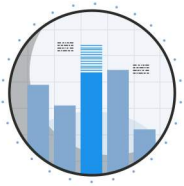
Аутсорсинг информационной безопасности

Компьютерная криминалистика (форензика)

Обучение информационной безопасности



Пентест (тест на проникновение)



Сертификация

Введение систем информационной безопасности

Разработка безопасного ПО