**КИБЕРБЕЗОПАСНОСТЬ**

**Риски безопасности информации и их классификация. Индустрия кибербезопасности. Кибербезопасность и контроль над Интернетом. Вредоносные приложения. Меры и средства защиты информации. Стандарты и спецификации в области информационной безопасности. Акты Республики Казахстан, регулирующие правоотношения в сфере информационной безопасности. Цифровая подпись. Кодирование.**

**Кибербезопасность. Риски безопасности информации и их классификация.**

Сегодня мы живем в один из самых трансформационных периодов в истории человечества, где все взаимосвязано. И эта связанная информационная сеть является неотъемлемой частью нашей повседневной жизни. Все организации, такие как государственные, медицинские, финансовые и образовательные учреждения, используют эту сеть для эффективной работы. Каждый день все эти организации собирают, обрабатывают, хранят и обмениваются огромным количеством цифровой информации. По мере сбора и распространения все большего количества цифровой информации, защита этой информации становится все более важной для нашей национальной безопасности и экономической стабильности.

Кибербезопасность - это усилия по защите компьютеров, серверов, мобильных устройств, электронных систем, сетей и всех находящихся на них данных от вредоносных атак. Сегодня все страны нуждаются в специалистах по кибербезопасности, чтобы помочь защитить своих граждан и инфраструктуру.

С развитием информационных и коммуникационных технологий и расширением доступа к Интернету организации становятся уязвимыми перед различными видами угроз. Угрозы исходят из разных источников, таких как кибератаки или деятельность сотрудников. Все люди или организации, которые хотят защитить свои данные или активы, должны знать риски, которым они подвержены, и распознавать их влияние, чтобы определить, что им необходимо сделать для предотвращения атак, выбрав соответствующие контрмеры.

Классификация рисков важна для организаций, так как является важным шагом на пути к обеспечению информационной безопасности. Риск может быть вызван внутренними и внешними объектами.

Внутренние риски возникают, когда кто-то имеет доступ к сети посредством учетной записи на сервере или физического доступа к сети. Это может быть результатом действий сотрудника или сбоя организационного процесса.

Внешние риски исходят от людей или организаций за пределами компании. У них нет авторизованного доступа к компьютерной системе или сети. Стихийные бедствия, такие как землетрясения, наводнения и пожары, также относятся к внешним рискам. Внешние атаки происходят через подключенные сети, физическое вторжение или партнерскую сеть.

Классификацию рисков, основанную на безопасности информационной системы, можно разделить на следующие виды:

1. Заблуждения и упущения - это вид угрозы безопасности, который обычно вызывается человеческими ошибками.

2. Мошенничество и кража - это вид угрозы безопасности, который может быть осуществлен с использованием различных современных форм мошенничества и кражи.

3. Саботаж сотрудника - это вид угрозы безопасности, когда человек, работающий в компании, подвергает риску ресурсы информационной системы.

4. Потеря физической инфраструктуры - это вид угрозы безопасности, который может быть вызван отключением электроснабжения, потерей связи, наводнением, пожаром, землетрясением, забастовками и т.д.

5. Хакеры - это вид угрозы безопасности, когда люди несанкционированным способом пытаются получить доступ и использовать системные ресурсы.

6. Вредоносное ПО - это вид угрозы безопасности, который включает в себя различные типы компьютерных вирусов, троянских программ, червей, логических бомб и других форм «нежелательного» программного обеспечения.

7. Угрозы личной конфиденциальности - это вид угрозы, когда множество личных данных может быть не по назначению использовано разными способами.

**Кибербезопасность и контроль над Интернетом**

Сегодня социальные сети меняют роль Интернета. В первое время мы могли контролировать наше поведение в Интернете и имели возможность быть тем, кем мы хотели быть. Мы могли выбирать и решать, какими особенностями делиться с другими. В настоящее время, поскольку Интернет начал расти с каждым днем, его трудно контролировать. Наша оффлайн-идентичность напрямую связана с нашими онлайн-действиями. История нашего интернет-браузера, поисковых запросов и посещений веб-страниц, электронной почты и социальных сетей несут в себе определенные признаки нашей личности.

Ваша онлайн-идентичность - это то, кем вы являетесь в киберпространстве. Это то, как вы представляете себя другим людям в Интернете. И вы должны быть аккуратны с личной информацией в Интернете. Ваше имя пользователя не должно заставлять незнакомцев думать, что вы - легкая мишень для киберпреступлений или нежелательного внимания.

Вся информация о вас может считаться вашими данными. Она включает в себя все фотографии и сообщения, которыми вы обмениваетесь со своей семьей, друзьями или коллегами. Медицинская, образовательная, финансовая, информация по вопросам занятости также может быть использована для идентификации вас в Интернете. Существует много информации о нас и разные законы, которые защищают нашу конфиденциальность и данные, но мы не знаем, где находятся все наши данные.

**Вредоносные программы (вирус)**

Вирус - это вредоносное программное обеспечение, которое можно использовать для кражи данных. Он может принимать форму исполняемого кода, скриптов, активного контента и другого программного обеспечения. Такие коды описываются как компьютерные вирусы, черви, троянские кони, рекламное ПО, боты, программы-вымогатели и т.д.

*Компьютерный вирус* - Вирус - это вредоносный исполняемый код, который прикрепляется к другим исполняемым файлам, часто легальным программам.

*Черви* - Черви представляют собой вредоносный код, который копирует себя, независимо используя уязвимости в сетях. Они обычно замедляют работу сетей.

*Троянские кони* - Троянский конь - это вредоносная программа, которая выполняет вредоносные операции под видом желаемой операции.

*Рекламное ПО* - Рекламное ПО - это вредоносная программа, которая генерирует онлайн-рекламу в пользовательском интерфейсе программного обеспечения.

*Бот* - Бот - это вредоносная программа, предназначенная для автоматического выполнения действий, как правило, в Интернете.

*Программа-вымогатель* - Программа-вымогатель - это вредоносная программа, предназначенная для удержания компьютерной системы или содержащихся в ней данных до тех пор, пока не будет произведена оплата.

*Атака "отказ в обслуживании" (DoS)* - это вид сетевой атаки. Она отключает сеть и делает ее недоступной для предполагаемых пользователей. Существует два основных метода DoS-атак: "затопление" либо "сбой".

"Затопление" - происходит, когда атакуемая система перегружена большим объемом трафика, который сервер не в состоянии обработать.

"Сбой" - происходит, когда киберпреступники передают ошибки, которые используют недостатки в целевой системе.

*Распределенная атака «отказ в обслуживании» (DDoS)* похожа на DoS-атаку, но исходит из нескольких координирующих источников. Она происходит, когда несколько систем организуют синхронизированную DoS-атаку на одну цель.

*Фишинг* - это киберпреступление, при котором с целью или целями связываются по электронной почте, телефону или текстовому сообщению. Например, электронное письмо от розничного магазина с просьбой перейти по ссылке, чтобы получить приз. Ссылка может перевести на фальшивый сайт с просьбой предоставить личную информацию либо этот сайт может установить вирус.

Как вы можете определить, что ваша система заражена вредоносными программами? Ниже приведены несколько признаков заражения вредоносными программами:

* Компьютер тормозит
* Файлы изменены или удалены
* Сбои
* Наличие неизвестных файлов, программ или значков на рабочем столе
* Запуск неизвестных процессов
* Ошибки браузера
* Увеличение интернет-трафика
* Письма отправляются без вашего ведома

**Меры и средства защиты информации**

Чтобы защитить информацию и личные данные, вам необходимо следовать простым важным шагам:

* Включите брандмауэр вашего компьютера. Брандмауэр - это уровень безопасности, который определяет, какой трафик может, а какой не может входить в ваш компьютер из сети. Как правило, он пропускает хороший трафик, исключая при этом хакеров, вредоносное ПО и другой сомнительный трафик.
* Используйте антивирус. Антивирусное программное обеспечение предназначено для сканирования вашего компьютера и удаления вирусов. Способы распространения вирусов через электронную почту – открытие вложения в электронном письме, посещение зараженного веб-сайта, нажатие на исполняемый файл или просмотр зараженной рекламы.
* Управляйте своей операционной системой и браузером. Хакеры всегда пытаются воспользоваться уязвимыми местами в ваших операционных системах и веб-браузерах. А для защиты ваших данных вам необходимо обновить операционные системы, в том числе веб-браузеры, попытаться установить последние версии программного обеспечения.
* Защитите все ваши устройства. Ваша компьютерная техника, будь то ПК, ноутбуки, планшеты, смартфоны, должна быть защищена паролем для предотвращения несанкционированного доступа. И никогда не используйте одинаковый пароль для всех ваших устройств.
* Зашифруйте свои данные. Шифрование - это процесс преобразования информации из легко читаемого и понятного формата в форму, которую несанкционированная сторона не может прочитать. На рынке представлены инструменты шифрования, которые предназначены для шифрования файлов, папок и даже целых драйверов.

При выборе инструментов шифрования следует учитывать следующее:

1. Цель шифрования, например, файлы, электронные письма и т.д.
2. Эксплуатационные требования
3. Обработка временных файлов
4. Простота развертывания
5. Простота использования
6. Управление и восстановление ключей

Вы можете зашифровать свои данные с помощью Шифрованной файловой системы (EFS) во всех версиях Windows, следуя следующим инструкциям:

1. Выберите один или несколько файлов либо папок.
2. Щелкните правой кнопкой мыши на выбранных данных >Свойства.
3. Нажмите на Дополнительно...
4. Установите флажок Зашифровать содержимое для защиты данных.
5. Файлы и папки, зашифрованные с помощью EFS, отображаются зеленым цветом, как показано на рисунке.

В настоящее время популярные онлайн-сервисы, такие как Google, Facebook, Twitter используют двухфакторную аутентификацию, чтобы обеспечить дополнительный уровень безопасности для входа в аккаунт. Помимо имени пользователя и пароля, персонального идентификационного номера (PIN) или шаблона, для двухфакторной аутентификации требуется второй опознавательный знак, как, например:

* Физический объект - кредитная карточка, карточка ATM, телефон, или ключ-карта
* Биометрическое сканирование - отпечаток пальца, отпечаток ладони, а также распознавание лица или голоса

Брандмауэр - это система сетевой безопасности, которая проверяет и контролирует входящий и исходящий сетевой трафик на основе предопределенных правил безопасности. Он может быть установлен на компьютере с целью защиты этого компьютера (локальный брандмауэр), или это может быть сетевое устройство, которое защищает сеть компьютеров и все хост-устройства в этой сети.

Виды брандмауэра:

* Сетевой или пакетный брандмауэр, осуществляющий фильтрование на основе сетевых адресов, портов или протоколов
* Брандмауэр приложений, осуществляющий фильтрование на основе приложений, программ или служб
* Брандмауэр прокси-сервера, осуществляющий фильтрование клиентских запросов на подключение
* Брандмауэр преобразования сетевых адресов включает в себя большую частную сеть, использующую адреса в частном диапазоне
* Локальный брандмауэр, осуществляющий фильтрование портов и вызовов системных служб в операционной системе одного компьютера.

Виртуальная частная сеть (VPN) - это служба, которая позволяет безопасно и конфиденциально получать доступ к сети, маршрутизируя соединение через сервер и скрывая свои действия в интернете. Эта служба шифрует ваши данные, и онлайн-адресат видит ваши данные как поступающие из VPN, а не с вашего компьютера и вашего местоположения.

**Стандарты и спецификации в области информационной безопасности**

В сущности, стандарт, будь то стандарт подотчетности, технический стандарт или стандарт информационной безопасности, представляет собой набор требований, которым должен соответствовать продукт или система. Потребность в стандартах в области информационной безопасности была признана на протяжении длительного времени и в последние годы значительно развивалась. Сначала была опубликована знаменитая Оранжевая Книга ”Критерии оценки доверенных компьютерных систем" Министерства обороны США. Другие важные стандарты этих лет включают в себя: "Руководящие документы Государственной технической комиссии Российской Федерации», «Критерии оценки безопасности информационных технологий (ITSEC)», «Стандарты классификации безопасности федеральной информации и информационных систем», "Канадские критерии оценки доверенной компьютерной продукции".

В последние годы в разных странах появилось новое поколение стандартов, посвященных практическим вопросам управления информационной безопасностью компании. В первую очередь, это международные стандарты управления информационной безопасностью ISO15408, ISO17799 и др.

Стандарт ISO/IEC17799: 2002 является одним из самых известных стандартов в области информационной безопасности. В нем рассматриваются следующие вопросы обеспечения информационной безопасности организаций и предприятий:

* необходимость обеспечения информационной безопасности
* основные понятия и определения информационной безопасности
* политика информационной безопасности компании
* классификация и управление корпоративными информационными ресурсами
* управление персоналом и информационная безопасность
* физическая безопасность
* администрирование безопасности информационных систем
* управление доступом
* требования безопасности для ИС в случае разработки, эксплуатации и технического обслуживания

Среди различных стандартов информационной безопасности, которые в настоящее время существуют в Казахстане, следует выделить нормативные документы по критериям оценки безопасности компьютерной техники и документы, регламентирующие информационную безопасность. К ним относятся нормативные документы по криптографической защите систем обработки информации и информационных систем. Ниже приведен список некоторых из этих стандартов:

* СТРК 34.026-2006 Защита информации. Термины и определения.
* СТРК 34.022-2006 Защита информации. Требования к проектированию, установке, наладке, эксплуатации и обеспечению безопасности информационных систем.
* CT PK 34.023-2006 Информационные технологии. Методы оценки соответствия информационных систем требованиям безопасности.
* CT PK ГОСТ Р 50739-2006 Вычислительная техника. Защита информации от несанкционированного доступа. Общие технические требования
* CT PK ИСО/МЭК 14888-3-2006 Информационные технологии. Методы защиты информации. Цифровые подписи через приложение. Часть 3. Механизмы на основе сертификатов

**Акты Республики Казахстан, регулирующие правоотношения в сфере информационной безопасности. Цифровая подпись. Кодирование.**

Общение в мессенджерах, онлайн платежи, электронные услуги – все это становится частью повседневности современного человека. Цифровизация, которая интенсивно вошла в жизнь казахстанцев с принятием государственной программы "Цифровой Казахстан", создает новую модель экономики, в которой оцифровываются не только основные отрасли и бизнес, но и вся жизнь общества.

Например, eGov.kz портал электронного правительства работает для того, чтобы граждане имели быстрый доступ к государственным услугам. Это такие услуги, как подача заявок, получение сертификатов, лицензий, регистрация и другие операции. Все эти операции могут быть подписаны вашей цифровой подписью.

Цифровая подпись - это тип электронной подписи, основанный на стандартах инфраструктуры открытых ключей (PKI), позволяющий пользователям подписывать документы в соответствии с правилами страны. Цифровая подпись часто используется для реализации электронной подписи, которая включает любые электронные данные, несущие в себе намерение подписи. 7 января 2003 года правительство Казахстана приняло закон "Об электронном документе и электронной цифровой подписи".