Тема лекции 14. Информационная безопасность оказания онлайн услуг

1. **Информационная безопасность: понятие и содержание.**
2. **Принципы информационной безопасности.**
3. **Кибербезопасность оказания онлайн услуг.**

4. Информационная безопасность - это комплекс мер, которые нужны, чтобы защитить от утечки или взлома программы, компьютерные системы и данные. Еще так называют отрасль, которая занимается этими мерами.

Простой пример меры по информационной безопасности - антивирус, установленный на компьютере. Но в коммерческих структурах к этому вопросу подходят более серьезно и на многих уровнях: чтобы обеспечить безопасность, нужно много чего сделать.

Средства информационной безопасности защищают данные от утечки, программы, системы и сети - от взлома, несанкционированного доступа, порчи файлов или других видов атак. Если речь о коммерческих или государственных структурах, сведения также защищают от шпионов или возможных злоумышленников внутри самого коллектива.

Информационная безопасность защищает системы от проникновения и от атак. Сюда входит не только взлом: это и DDoS-атаки, в результате которых может «лечь» сервер сайта, и утечка данных, и многое другое. Злоумышленников намного больше, чем кажется. И никто не хочет, чтобы их сервис потерял работоспособность, а данные оказались доступны всем вокруг. Для этого и нужна информационная безопасность.

У компаний есть еще одна причина: за утечку конфиденциальных данных пользователей они несут ответственность по закону. Так что для них меры по безопасности - это еще и способ избежать проблем с законодательством и потери доверия клиентов.

Без мер по информационной безопасности кто угодно мог бы получить доступ к конфиденциальным сведениям или взломать любой сайт или систему. Компьютерным пространством стало бы фактически невозможно пользоваться.

Угрозы безопасности разделяют на две категории: внутренние и внешние.

Внутренние. Это угрозы, которые идут изнутри системы. Чаще всего в таких случаях речь идет об утечке данных или об их повреждении. Например, кто-то подкупил сотрудника, и тот похитил данные, составляющие коммерческую тайну. Второй вариант - злоумышленником оказался авторизованный пользователь.

Еще одна внутренняя угроза - риск банальной ошибки, в результате которой конфиденциальные сведения окажутся в открытом доступе или повредятся. Например, в открытом доступе оказалась часть базы данных или пользователь по неосторожности повредил файлы. Такое уже бывало в истории. А нужно, чтобы таких случаев не возникало: клиент не мог бы

нарушить работу системы даже случайно, а информация оставалась защищена.

Внешние. Сюда относятся угрозы, которые приходят извне, и они могут быть куда разнообразнее. Это, например, попытка взлома системы через найденную уязвимость: злоумышленник проникает в сеть, чтобы украсть или повредить информацию. Или DDoS-атака, когда на веб-адрес приходит огромное количество запросов с разных адресов, и сервер не выдерживает, а сайт перестает работать.

Сюда же можно отнести деятельность компьютерных вирусов: они способны серьезно навредить работе системы. Действия таких вредоносных программ могут быть очень разнообразными: от рассылки спама от имени взломанного адреса до полной блокировки системы и повреждения файлов.

Еще к внешним угрозам безопасности относятся форс-мажоры и несчастные случаи. Например, хранилище данных оказалось повреждено в результате аварии или пожара. Такие риски тоже нужно предусмотреть.

Существует отдельная должность специалиста по информационной безопасности. В крупных компаниях это может быть отдельный департамент. В маленьких - один сотрудник, причем порой он также выполняет обязанности системного администратора или сетевого инженера. Бывает и так, что информационную безопасность отдают на аутсорс: в этом случае ею занимаются сотрудники специализированной компании.

В широком смысле простейшие меры по информационной безопасности предпринимает кто угодно. Установить антивирус и блокировщик навязчивой рекламы, не посещать подозрительные сайты и не запускать непроверенные файлы - все это тоже меры ИБ, хоть и максимально простые. Но настоящий специалист по безопасности - это профессионал с широкими знаниями и множеством специфических навыков.

2. Три принципа информационной безопасности

Информационная безопасность отвечает за три вещи: доступность, конфиденциальность и целостность данных. Сейчас расскажем, что это означает.

Доступность. Это значит, что к информации могут получить доступ те, у кого есть на это право. Например, пользователь может зайти в свой аккаунт и увидеть все, что в нем есть. Клиент может перейти в каталог и посмотреть на товары. Сотрудник может зайти во внутреннюю базу данных для его уровня доступа. А если на систему производится атака и она перестает работать, доступность падает порой до полного отказа.

Конфиденциальность. Второй принцип - конфиденциальность. Он означает, что информация должна быть защищена от людей, не имеющих права ее просматривать. То есть в тот же аккаунт пользователя не сможет войти чужой человек. Без регистрации нельзя комментировать что-то на сайте, без личного кабинета - оплатить заказ. Человек, который не работает в компании, не может зайти в ее внутреннюю сеть и посмотреть там на конфиденциальные данные. Если систему взламывают, конфиденциальность оказывается нарушенной.

Целостность. Целостность означает, что информация, о которой идет речь, не повреждена, существует в полном объеме и не изменяется без ведома ее владельцев. Комментарий не сможет отредактировать посторонний человек - только автор или иногда модератор. Сведения в базе данных меняются только по запросу тех, у кого есть доступ. А в вашем аккаунте не появятся письма, написанные от вашего лица без вашего ведома. При взломе системы целостность опять же может нарушиться: информацию могут модифицировать, повредить или стереть.

В казахстанском сегменте интернета 150 тысяч доменных имен. Комитет информационной безопасности РК разработал приложение Web Totem. Это казахстанская разработка, позволяющая ставить сайт под определенную защиту. Если на сайтах будут выявляться уязвимости, владелец сайта получит оповещение о том, что нужно предпринимать меры. Это сервис по уведомлению населения об использовании персональных данных.

3. Кибербезопасность (ее иногда называют компьютерной безопасностью) – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных. Кибербезопасность находит применение в самых разных областях, от бизнес-сферы до мобильных технологий. В этом направлении можно выделить несколько основных категорий.

Кибербезопасность – это деятельность, нацеленная на обеспечение защиты пользователей, их информационных систем, сетей, и программ от цифровых атак.

Основной целью таких кибератак может являться как получение конфиденциальной информации пользователя для дальнейшего злоупотребления этой информации в собственных целях хакера, так и нарушение работы целого бизнес-процесса. Поэтому, в особенности контекста государственных подразделений и больших частных организаций, для Казахстана как и для других стран мира одной из основных задач для эффективного и безопасного присутствия в интернете является именно развитие сферы кибербезопасности.

КОНЦЕПЦИЯ «КИБЕРЩИТ»

Целью Концепции «КИБЕРЩИТ Казахстана» является достижение и поддержание уровня защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз, обеспечивающего устойчивое развитие Республики Казахстан в условиях глобальной конкуренции (О концепции «Киберщит»).

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ (DATA PROTECTION AGENCY)

Общий регламент о защите данных (правила по обработке линых данных) является законом прямого действия в 28 странах Евросоюза. На

основании общего регламента будет функционировать организация по Защите персональных данных (Data protection agency) в Казахстане.

- **Безопасность сетей**– действия по защите компьютерных сетей от различных угроз, например целевых атак или вредоносных программ.
- **Безопасность приложений**– защита устройств от угроз, которые преступники могут спрятать в программах. Зараженное приложение может открыть злоумышленнику доступ к данным, которые оно должно защищать. Безопасность приложения обеспечивается еще на стадии разработки, задолго до его появления в открытых источниках.
- **Безопасность информации**– обеспечение целостности и приватности данных как во время хранения, так и при передаче.
- **Операционная безопасность**– обращение с информационными активами и их защита. К этой категории относится, например, управление разрешениями для доступа к сети или правилами, которые определяют, где и каким образом данные могут храниться и передаваться.
- **Аварийное восстановление и непрерывность бизнеса** – реагирование на инцидент безопасности (действия злоумышленников) и любое другое событие, которое может нарушить работу систем или привести к потере данных. Аварийное восстановление – набор правил, описывающих то, как организация будет бороться с последствиями атаки и восстанавливать рабочие процессы. Непрерывность бизнеса – план действий на случай, если организация теряет доступ к определенным ресурсам из-за атаки злоумышленников.
- **Повышение осведомленности**– обучение пользователей. Это направление помогает снизить влияние самого непредсказуемого фактора в области кибербезопасности – человеческого. Даже самая защищенная система может подвергнуться атаке из-за чьей-то ошибки или незнания. Поэтому каждая организация должна проводить тренинги для сотрудников и рассказывать им о главных правилах: например, что не нужно открывать подозрительные вложения в электронной почте или подключать сомнительные USB-устройства.

Виды киберугроз

Кибербезопасность борется с тремя видами угроз.

1. **Киберпреступление**– действия, организованные одним или несколькими злоумышленниками с целью атаковать систему, чтобы нарушить ее работу или извлечь финансовую выгоду.
2. **Кибератака** – действия, нацеленные на сбор информации, в основном политического характера.
3. **Кибертерроризм** – действия, направленные на дестабилизацию электронных систем с целью вызвать страх или панику.

Как злоумышленникам удается получить контроль над компьютерными системами? Они используют различные инструменты и приемы – ниже мы приводим самые распространенные.

Вредоносное ПО

Название говорит само за себя. Программное обеспечение, которое наносит вред, – самый распространенный инструмент киберпреступников. Они создают его сами, чтобы с его помощью повредить компьютер пользователя и данные на нем или вывести его из строя. Вредоносное ПО часто распространяется под видом безобидных файлов или почтовых вложений. Киберпреступники используют его, чтобы заработать или провести атаку по политическим мотивам.

Вредоносное ПО может быть самым разным, вот некоторые распространенные виды:

- **Вирусы –** программы, которые заражают файлы вредоносным кодом. Чтобы распространяться внутри системы компьютера, они копируют сами себя.
- **Троянцы–** вредоносы, которые прячутся под маской легального ПО. Киберпреступники обманом вынуждают пользователей загрузить троянца на свой компьютер, а потом собирают данные или повреждают их.
- **Шпионское ПО –** программы, которые втайне следят за действиями пользователя и собирают информацию (к примеру, данные кредитных карт). Затем киберпреступники могут использовать ее в своих целях.
- **Программы-вымогатели** шифруют файлы и данные. Затем преступники требуют выкуп за восстановление, утверждая, что иначе пользователь потеряет данные.
- **Рекламное ПО –** программы рекламного характера, с помощью которых может распространяться вредоносное ПО.
- **Ботнеты –** сети компьютеров, зараженных вредоносным ПО, которые киберпреступники используют в своих целях.

SQL-инъекция

Этот вид кибератак используется для кражи информации из баз данных. Киберпреступники используют уязвимости в приложениях, управляемых данными, чтобы распространить вредоносный код на языке управления базами данных (SQL).

Фишинг – атаки, цель которых – обманом заполучить конфиденциальную информацию пользователя (например, данные банковских карт или пароли). Часто в ходе таких атак преступники отправляют жертвам электронные письма, представляясь официальной организацией.

Атаки Man-in-the-Middle («человек посередине»)

Это атака, в ходе которой киберпреступник перехватывает данные во время их передачи – он как бы становится промежуточным звеном в цепи, и жертвы об этом даже не подозревают. Вы можете подвергнуться такой атаке, если, например, подключитесь к незащищенной сети Wi-Fi.

DoS-атаки (атаки типа «отказ в обслуживании»)

Киберпреступники создают избыточную нагрузку на сети и серверы объекта атаки, из-за чего система прекращает нормально работать и ею становится невозможно пользоваться. Так злоумышленники, например,

могут повредить важные компоненты инфраструктуры и саботировать деятельность организации.

Вопросам развития сферы кибербезопасности в Казахстане уделяется пристальное внимание. И результат работы, проводимой совместно государственными органами, НПО и бизнесом – это тенденция последних лет, когда наша страна стремительно улучшает свои позиции в глобальном индексе кибербезопасности. Сейчас Казахстан занимает в нём 40-е место. Отметим, что ещё в прошлом году наша страна находилась на 42 пункта ниже, занимая 82 место.

За прошедшие годы в стране были выработаны базовые концептуальные подходы к развитию сферы кибербезопасности страны. Разработана и уже утверждена концепция кибербезопасности "Киберщит Казахстана", действие которой рассчитано до 2022 года. Вместе с тем уже вступил в действие целый ряд законодательных актов и большое количество отраслевых приказов. Помимо этого, созданы испытательные лаборатории в сфере информационной безопасности по исследованию вредоносного кода, запущен национальный координационный центр информационной безопасности, частная служба реагирования на компьютерные инциденты (CERT), 7 оперативных центров информационной безопасности (SOC), увеличено число грантов по этой специальности и т.д.

Для дальнейшего улучшения ситуации в сфере информационной безопасности и защите персональных данных, Министерством цифрового развития, инноваций и аэрокосмической промышленности РК инициирован вопрос о наделении Комитета по информационной безопасности функциями по защите персональных данных, проведения аудита и проверок владельцев информационных систем, в которых обрабатываются персональные данные.

Контрольные вопросы:

1. Информационная безопасность: понятие и содержание.
2. Принципы информационной безопасности.
3. Кибербезопасность оказания онлайн услуг.
4. Виды угроз.
5. Система безопасности оказания онлайн услуг.