АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИССЛЕДУЕМОЙ СИСТЕМЕ ПРЕДПРИЯТИЯ/ОРГАНИЗАЦИИ

Жанабаев Арысланбек
студент
Нукусский филиала Ташкентского университета информационных технологий имени Мухаммада аль-Хорезми

Аннотация: *В современном мире, где информационные технологии занимают центральное место в деятельности предприятий и организаций, вопросы обеспечения информационной безопасности становятся все более актуальными. В последние годы участились случаи кибератак, утечек данных и прочих инцидентов, связанных с информационной безопасностью, что может приводить к значительным финансовым и репутационным потерям. В условиях глобальной цифровизации и растущей зависимости бизнеса от информационных систем, анализ угроз информационной безопасности является критически важным для обеспечения устойчивой и безопасной работы предприятий.*

Ключевые слова: *методы анализа угроз, правовые и нормативные акты в области информационной безопасности, конфиденциальность, целостность, доступность информации в предприятии.*

Сегодня проблема обеспечения безопасности корпоративной сети является очень важной и должна решаться, начиная с этапа проектирования топологии сети. Таким образом, в последние годы область информационной безопасности значительно выросла и эволюционировала. Она предлагает множество областей для специализации, включая обеспечение безопасности сетей и смежной инфраструктуры, защиту приложений и баз данных, тестирование безопасности, аудит информационных систем, планирование непрерывности бизнеса и т.д.

Информационная безопасность (ИБ) представляет собой совокупность мер и процессов, направленных на защиту информационных систем, данных и ресурсов от различных угроз. Основная цель ИБ – достижение состояния защищенности информации, обеспечивающее ее конфиденциальность, целостность и доступность. Это три ключевых принципа информационной безопасности, часто обозначаемые как триада CIA (Confidentiality, Integrity, Availability), на рис.1. показаны ключевые принципы информационной безопасности.

Конфиденциальность подразумевает защиту информации от несанкционированного доступа и разглашения. Основные методы обеспечения конфиденциальности включают:

- Шифрование: Преобразование информации в код, который может быть прочитан только с помощью ключа расшифровки. Шифрование защищает данные как при передаче, так и при хранении, гарантируя, что только авторизованные лица могут

получить доступ к содержимому. Примеры технологий шифрования включают симметричное шифрование (например, AES) и асимметричное шифрование (например, RSA).

- Системы контроля доступа: Установление прав и привилегий для пользователей, что ограничивает доступ к информации только авторизованным лицам. Контроль доступа может быть основан на ролевой модели (RBAC), мандатной модели (MAC) или дискреционной модели (DAC). Например, сотрудники отдела кадров могут иметь доступ к личным данным сотрудников, в то время как другие отделы такой доступ не имеют.
- Аутентификация и авторизация: Процессы проверки подлинности пользователя (аутентификация) и определения его прав доступа к ресурсам (авторизация). Аутентификация может осуществляться с помощью паролей, биометрических данных (например, отпечатков пальцев) или многофакторной аутентификации (например, комбинации пароля и одноразового кода). Авторизация определяет, какие действия пользователь может выполнять после успешной аутентификации.

Целостность гарантирует точность и полноту информации, защищая ее от несанкционированного изменения. Методы обеспечения целостности включают:

- Контрольные суммы и хеш-функции: Использование алгоритмов для создания уникальных идентификаторов данных, которые изменяются при любом изменении информации. Например, хеш-функции (MD5, SHA-256) создают хеш-значения, которые можно проверить для удостоверения целостности данных.
- Цифровые подписи: Механизмы, обеспечивающие проверку подлинности и целостности данных, подписанных авторизованным пользователем. Цифровые подписи используют асимметричное шифрование для создания и проверки подписей, гарантируя, что данные не были изменены после их подписания.
- Резервное копирование: Создание копий данных для восстановления в случае их повреждения или утраты. Регулярное резервное копирование и проверка восстановимых копий являются критически важными для обеспечения целостности данных.

Рис.1. Ключевые принципы информационной безопасности

Доступность обеспечивает возможность доступа к информации для авторизованных пользователей в нужное время. Это требует мер по предотвращению отказов в обслуживании и обеспечения бесперебойной работы систем, таких как:

- Резервные системы и аварийное восстановление: Поддержание резервных копий и планов восстановления после сбоев. Это включает в себя создание аварийных центров данных и регулярное тестирование планов восстановления для обеспечения минимальных простоев.
- Системы распределения нагрузки: Распределение запросов пользователей между несколькими серверами для предотвращения перегрузки. Балансировка нагрузки помогает распределить трафик и обеспечить устойчивую работу систем даже при высоких нагрузках.
- Антивирусные и анти-DDoS меры: Использование программного обеспечения для защиты от вредоносных программ и атак на отказ в обслуживании. Антивирусные программы сканируют и удаляют вредоносное ПО, а анти-DDoS системы помогают защитить сети от массовых атак, направленных на их перегрузку.

Информационная безопасность является неотъемлемой частью управления современными предприятиями и организациями. Эффективное управление ИБ помогает предотвратить финансовые потери, сохранить репутацию компании и обеспечить выполнение правовых и регуляторных требований. В условиях постоянно меняющихся угроз и технологий, предприятия должны регулярно пересматривать и обновлять свои стратегии и меры безопасности для поддержания высокого уровня защиты информации.

Схема офиса предприятия ООО «DATA KARSU»

Компания «DATA KARSU», которая занимается разработкой ПО, зарекомендовавшая себя как компания с высококвалифицированными специалистами, имеющая отличную профессиональную репутацию. «DATA KARSU» сотрудничает с компаниями различных видов деятельности, как с предприятиями государственного сектора, так и коммерческими организациями, например, строительные компании, различные холдинги, филиалы.

На предприятии работают 94 сотрудника, в их число входят:

- директор: 1 человек;
- заместители директора: 2 человека;
- отдел кадров: 4 человек;
- бухгалтерия: 4 человек;
- IT специалист: 4 человек;
- отдел по работе с клиентами: 15 человек;
- налоговый сектор: 20 человек;
- аудиторы: 20 человек;
- сектор бухгалтерских услуг: 15 человек;
- кассир: 2 человека;
- служба безопасности: 4 человека (посменно);

Здание предприятия состоит из трех этажей. Ниже на рисунках представлена внутренняя инфраструктура предприятия.

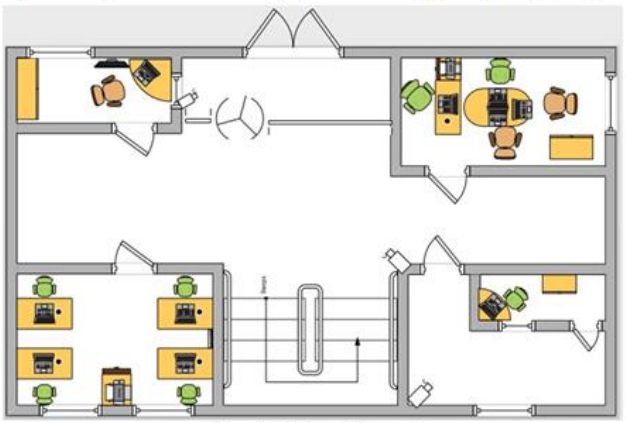

Рис.2. План 1 этажа

На первом этаже находятся кабинеты: службы безопасности, бухгалетерии, кассы и HR менеджеров. На втором этаже находятся кабинеты: руководителя и его заместителей, IT специалистов, сектора бухгалтерских услуг. На третьем этаже находятся кабинеты: отдела по работе с клиентами, налогового сектора и аудиторов.

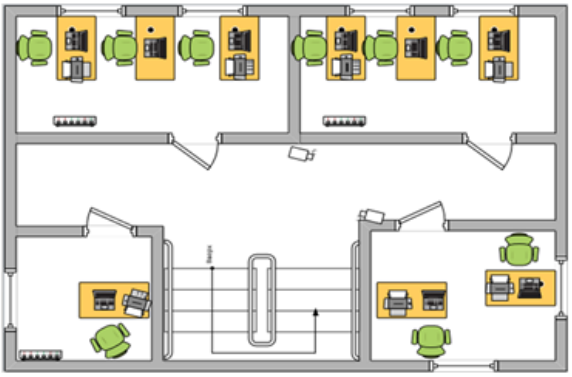

Рис.3. План 2 этажа

Многие компании акцентируют внимание на информационной безопасности, но часто пренебрегают обеспечением необходимого уровня физической безопасности. Информационная безопасность это и есть понятие комплексное, и эффективную информационную безопасность почти невозможно реализовать без надежной физической защиты. Физическая безопасность - это меры, которые входят в состав обеспечения комплексной безопасности и направленные на создание системы защиты организации, активов и персонала от внешних угроз и злонамеренных действий физических лиц. Это технические средства охраны предприятия, сотрудники, обеспечивающие безопасность организации, действующая режимная (пропускная) система охраны организации.

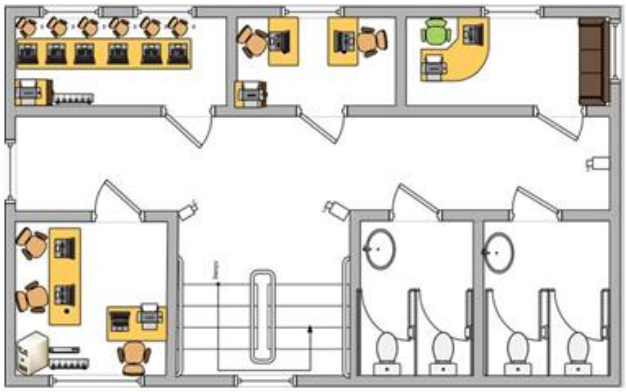

Рис.4. - План 3 этажа

Обычно предприятия используют системы для контроля и управления доступом для организации физической защиты. Эта технология может быть реализована с помощью различных способов. Часто применяемый способ - бесконтактные карты (смарт-карты). При использовании бесконтактных карт сотрудник, для получения доступа на территорию или в какое-либо помещение на предприятии использует ее для идентификации, и на основании сверки идентификатора, вшитого в нее, система проводит сравнение с эталоном, хранящимся в ее базе идентификаторов. На основе анализа выдает разрешение или запрещение на доступ. Системы СКУД имеют недостатки. Например, идентификационная карта может быть потеряна сотрудниками или они могут быть переданы другим людям. При утере смарт карт специалисты службы безопасности должны заблокировать ее и перевыпустить новую в замену ее, но в случае если она передана в чужие руки, то здесь возникают осложнения. Так как идентифицировать владельца карты может только человек. На пропускном пункте в системе должна отобразиться фотография владельца смарт-карты, когда тот проходит через систему контроля.

СКУД повышает уровень физической безопасности имущества охраняемого объекта. Программное обеспечение для управления доступом к дверям является неотъемлемой частью нашей системы контроля доступа. Это позволяет нам управлять дверными считывателями в нашей организации, а затем вводить и управлять всеми людьми, которые будут использовать двери.

Большая часть доступного программного обеспечения для управления доступом обеспечивает простое управление дверным считывателем. Мы можем контролировать, кто, когда и куда могут входить, либо выходить. Дополнительные функции позволяют определить, кто находится в здании, управлять системой с помощью мобильного устройства, заблокировать здание в чрезвычайной ситуации и многие другие функции.

Кто может войти в дверь, устанавливается, когда человеку присваиваются учетные данные и вводятся в систему управления. Учетный номер вводится вручную или путем считывания карты. В это время вводится имя человека, его уровень привилегий, возможно, его фотография и другая информация.

В ООО «DATA KARSU» службы безопасности находится на первом этаже следит за камерами видео наблюдения и фиксирует кто, когда заходил и выходил. Это не обеспечивает надежную безопасность информации внутри организации.

Сотрудники организации, чтобы войти в свой кабинет берут ключи от дверей у службы безопасности, то есть это также не обеспечивает достаточный уровень безопасности.

Существуют основные три аспекта информационной безопасности:

- конфиденциальность;
- целостность;
- доступность.

Обеспечение защиты данных от несанкционированного доступа начинается с момента попытки входа в систему. Операционная система должна проверить пользователя, входящего в систему, в том, что он имеет разрешение главного системного администратора инфраструктуры для входа в нее. Важным средством защиты данных являются функции аудита операционной системы, фиксирующего все происходящие события в системе, влияющие на ее безопасность. При этом администратор операционной системы определяет необходимый перечень событий для отслеживания.

Функции администрирования тесно взаимосвязаны с функциональностью защиты операционной системы, так как системный администратор инфраструктуры раздает права доступа пользователям при их обращении к различным ресурсам системы: либо файлам, либо каталогам, либо другим устройствам и т.д. Также, администратор для ограничения полномочий пользователей локальной сети в совершении каких-либо системных действий применяет функции групповых политик. Например, такие как запрещение смены даты, запрещение завершения работы какого-либо процесса, запрещение изменения прав доступа к различным ресурсам и т.п., Кроме того, системный администратор может также ограничить функциональность пользовательского интерфейса, например, удалить из меню операционной системы, отображаемые на мониторе пользователя какие-либо пункты.

Безопасность информационной системы заключается в обеспечении конфиденциальности, целостности и доступности информации, т.е. защиту информации от несакционнированного доступа, модификации, удаления, подмены и т.д.

На предприятии ООО «DATA KARSU», системные администраторы удаленно подключаются, используя ПО AnyDesk, чтобы настроить ПК пользователей. Это не совсем удобно и правильно. Для обеспечения определенного уровня защиты необходимо использовать службу каталогов Ac- tive Directory. Если внедрить эту систему, то можно предотвратить некоторые угрозы на информационную инфраструктуру и централизованно управлять всеми компьютерами дистанционно. В Active Directory, чтобы подключиться к контроллеру домена используется протокол Kerberos. Контроллер домена решает разрешить или запретить доступ к активным ресурсам предприятия, авторизуя и аутентифицируя конечных пользователей.

Сервера организации находятся в облаке и на физическом сервере, то есть к серверу есть постоянный доступ. Пароли для входа на удаленный рабочий стол выдает

системный администратор. Также ведется корпоративная почта от yandex, в которую системный администратор добавляет пользователей.

Также каждый пользователь может использовать средство шифрования BitLocker, который внедрен в каждую операционную систему. Использую ее можно шифровать жесткие диски, если в нем будут хранится секретные данные.

Таким образом, данное исследование позволило выявить ключевые угрозы информационной безопасности в исследуемой системе и предложить эффективные меры по их нейтрализации. Практическая значимость работы заключается в возможности применения разработанных рекомендаций для повышения уровня информационной безопасности в ООО «DATA KARSU» и других организациях с аналогичными проблемами.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. Seitnazarov K.K. Integration of gis technology for fuzzy deterministic simulation of conditions of operation and maintenance Kegeyli groundwater is abstracted// «IJRET» Volum 4 Issue 2. – Indiya, 2015. – P.727-735. eISSN: 2319-1163/pISSN: 2321-7308.
2. Усманов Р.Н., Сеитназаров К.К. Об организации параллельных вычислений в процессе решения геофильтрационных задач // Вестник ТУИТ. – Ташкент, 2014. - № 1. – С. 101-106. ISSN 2010-9857
3. Usmanov R.N., Seitnazarov K.K. The problem of information model development for the relationship between hydrogeological object and its fuzzy-deterministic model// The Advanced Science Journal. USA, 2014 –№7. – С.67-73. ISSN 2219-746X.
4. Усманов Р.Н., Сеитназаров К.К. Программный комплекс нечетко-детерминированного моделирования гидрогеологических объектов // Автоматика и программная инженерия. – Новосибирск, 2014. – № 1. – С. 29-34. ISSN 2312-4997.
5. Усманов Р.Н., Сеитназаров К.К. Нечетко-детерминированные математические модели процессов восстановления запасов и качества подземных вод // Наука и мир. – Волгоград, №5(21), 2015 – С. 102-104. ISSN 2308-4804.
6. К.К.Сеитназаров, Б.К.Туремуратова. Разница Между Глубоким И Машинным Обучением // Periodica Journal of Modern Philosophy, Social ..., 2022
7. К.К.Сеитназаров, Б.К.Туремуратова. ПРИМЕНЕНИЕ ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМЕ ДИСТАНЦИОННОГО ОБРАЗОВАНИЯ// Новости образования: исследование в XXI веке, 2022.
8. К.К. Сеитназаров, Д.Х. Турдышов, Б.К. Туремуратова. ОБЗОР МЕТОДОВ ПОЛУЧЕНИЯ КОСМИЧЕСКИХ ИЗОБРАЖЕНИЙ С ВЫСОКИМ РАЗРЕШЕНИЕМ// НАУКА и ОБЩЕСТВО
9. K. Seitnazarov, D. Turdishov, A. Dosimbetov. Knowledge base of algorithmic software complex for providing agricultural fields with water resources// AIP Conference Proceedings, 2024.

10. K.K. SEITNAZAROV, B.M. MAMBETKARIMOV. DEVELOPMENT AND APPLICATION OF A DIGITAL EDUCATIONAL RESOURCE FOR TEACHING PROGRAMMING IN HIGHER EDUCATION INSTITUTIONS// Mental Enlightenment Scientific-Methodological ..., 2024.

11. K.K. Seitnazarov, A.K. Bazarbaeva.METHODOLOGY FOR ASSESSING THE ECTS CREDIT SYSTEM IN HIGHER EDUCATIONAL INSTITUTIONS IN WESTERN EUROPE//Modern Science and Research 3 (2), 728-731.

12. К.К. Сеитназаров, Н.С. Мухиятдинов, М.М. Урынбаева. Искусственный интеллект и его применение в принятии решений: методы, алгоритмы и перспективы// Journal of Universal Science Research, 2023.

13. Seitnazarov K.K. Dosımbetov A.M., Aytanov A.K., Omaraov X./ Software Principles for Mapping the Relative State of Groundwater/ European Journal of Molecular & Clinical Medicine ISSN 2515-8260 Volume 7, Issue 11, 2020. – P 319-323.

14. Seitnazarov K.K. Dosımbetov A.M., Aytanov A.K/ Strategy for Organization of Computational Experiments of the Functioning of Underground Water Inlets Using a Fuzzy Multiple Approach/ 2020 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2020, pp. 1-4.

15. Seitnazarov K.K. Aytanov A.K.., Kojametov E., Asenbaev N./ 2021 International Conference on Information Science and Communications Technologies (ICISCT)./ Hydrogeological-Mathematical Model of Formation and Management of Resources and Quality of Fresh Underground Water of the Karakalpak Artesian Basin.