ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НА ПРЕДПРИЯТИИ СОВРЕМЕННЫЕ МЕТОДЫ ПОСТАВОК

Ташкентский государственный экономический университет
Старший преподаватель кафедры
Цифровая экономика и
информационные технологии
Юсупова Дильбар Мирабидовна

Аннотация: *В данной статье информационная безопасность на предприятиях в настоящее время мировой и национальный опыт предоставления Кроме того в статье рассматривается понятие информационной безопасности и ее сущность.*

Ключевые слова: *Информационная безопасность, угрозы, вирусы, спам, кибератаки.*

INFORMATSIONNAYA BEZOPASNOST NA PREDPRIYATII SOVRMENNYE METHODY POSTAVOK

Annotation: *In this state, the information security of enterprises and the current world and national experience are presented.*

Keywords: *Information security, threat, virus, spam, cyber attack.*

Сначала кратко прокомментируем понятие информационной безопасности. Информационная безопасность это практика защиты информации путем снижения информационных рисков. Это информация часть управления рисками. Обычно это неправомерный доступ к данным без разрешения или незаконное использование, раскрытие, нарушение, уничтожение, уничтожение, изменение, или, по крайней мере, предотвратить возможность проверки, записи или повреждения включает сокращение. Это тоже негативное влияние этих событий. включает в себя действия, направленные на снижение Любая защищенная информация может быть в форме, например электронный или физический. Обеспечение информационной безопасности Первые меры восходят к древним временам. Примером этого является следующее мы можем принести. Дипломаты и военные с первых дней общения в прошлом командиры любой механизм защиты конфиденциальности переписки осознали, что им необходимо иметь какие-то средства представления и идентификации. Примером этого является шифр Цезаря, изобретенный Юлием Цезарем. Этот шифр, созданный в 50 г. до н. э., предназначен для того, чтобы сделать секретные сообщения нечитаемыми. предназначен для предотвращения его попадания в чужие руки. В настоящее время угроза информационной безопасности на предприятиях обусловлена различными факторами. происходит в результате. Примером тому является внутренняя

информационная безопасность сотрудников компании. несоблюдение правил, выход из строя устройств приема и передачи информации, сюда входит различный спам и вирусные сообщения в Интернете. Из них существует несколько способов защиты, мы рассмотрим их ниже. Прежде всего, при обеспечении информационной безопасности на предприятии необходимо учитывать внутреннюю среду.

Особое внимание следует уделить управлению персоналом. Каждый сотрудник – это внутренний порядок предприятия правила должны соблюдаться безоговорочно. Мы можем привести следующие примеры. Сотрудники не должны раскрывать внутренние тайны компании. Это предпринимательское право должен соблюдать правила. Информационные устройства, которые сейчас используются на предприятии рассмотрим меры защиты от информационных угроз. Ни для кого не секрет, что Интернет сейчас в сети встречаются различные типы кибератак. В этом случае хакеры проникают в информацию компании. атаковать систему через Интернет и получить необходимую информацию. Например они используют информацию о номере банковского счета в своих целях. Теперь о том, как компьютерные вирусы и спам наносят ущерб информационной системе предприятия. давайте кратко остановимся на том, что это может принести. Это компьютерные вирусы представляет реальную угрозу современному бизнесу. Вирус на узлы корпоративной сети.

Проникновение может привести к нарушению их деятельности, потере рабочего времени, данных потеря, кража конфиденциальной информации и даже денег напрямую может привести к краже. Вирусная программа, проникающая в корпоративную сеть для хакеров. позволяет частично или полностью контролировать деятельность компании. Спам - это несколько за прошедшие годы спам превратился из незначительной неприятности в одну из крупнейших угроз безопасности. В последние годы электронная почта стала основным каналом распространения. Просматривайте спам-сообщения и потом на выключение уходит много времени, это создает у сотрудников ощущение психологического дискомфорта. Мы можем использовать антивирусные программы, чтобы избежать вирусов. Но это предприятие требует дополнительных затрат. Потому что сильные антивирусные программы платные. Из спама и защита заключается в том, что вы просто не открываете неизвестное сообщение электронной почты можно защитить. В настоящее время обеспечение информационной безопасности является одним из актуальных вопросов не только в деятельности компании, но и для представителей других отраслей, использующих информационные технологии. Поэтому обеспечение безопасности информации является очень важным вопросом для бесперебойного осуществления деятельности компании. Мы хотим продолжить наш разговор примером. Сегодня мы видим конкуренцию между предприятиями по всем направлениям. Каждая компания использует все свои возможности для победы в конкурентной борьбе. В качестве примера можно упомянуть, что компания держит в тайне стоимость производимой ею продукции. Если принять во внимание, что эта простая таблица хранится в виде

цифровой информации, мы не можем сказать, насколько важно для компании сохранить эту информацию в неприкосновенности. Кроме того, не секрет, что действующие в настоящее время крупные банки подвергаются атакам хакеров. Другой пример: сегодня вместе с информационными технологиями развиваются кибератаки и их виды увеличиваются. Особенно сейчас увеличивается количество кибератак с использованием социальной инженерии. Защита от них − один из актуальных вопросов современности. Приведем пример проблем, которые являются препятствием для обеспечения информационной безопасности в целом. В настоящее время к основным проблемам обеспечения информационной безопасности можно отнести обилие информации и сложность ее обработки. Обилие информационного потока серьезно затрудняет его защиту. И одна из главных проблем — определить, какую информацию следует защищать. Одной из главных проблем безопасности является отсутствие единой системы безопасности. Как мы упоминали ранее, экономическая эффективность процесса управления информационной безопасностью организации во многом зависит от того, что необходимо защитить. В заключение можно сказать, что в настоящее время на предприятии отсутствует информация защита является одним из основных факторов, обеспечивающих бесперебойную работу предприятия Считается Предприятие теперь современно в области информационной безопасности аппаратное и программное обеспечение может помочь. Мы делаем это с помощью следующих мы можем объяснить. Просто с устройства распознавания лиц на территории предприятия Использование может оказаться весьма эффективным в обеспечении информационной безопасности предприятия. Но использование таких инструментов может потребовать дополнительных затрат для предприятия. Кроме того, можно также электронно установить ключевые слова на электронные устройства на предприятии. Это эффективно защищает данные, хранящиеся таким образом. Теперь кратко коснемся системы информационной безопасности предприятия. Организация система информационной безопасности включает в себя следующие направления; нормативный, организационный (административное), техническое, программное обеспечение. Каждая сеть должна быть тесно связана друг с другом нуждаться они неразрывно связаны. Информация для полной оценки ситуации по всем направлениям безопасности на предприятии и цели, определяющие системный подход к проблеме ресурсной безопасности, разработка концепции информационной безопасности, в которой системно представлены задачи нуждаться конечно, это процесс, который требует времени и денег. Задача обеспечения информационной безопасности должна решаться системно. Вот и все означает, что различные средства защиты (аппаратные, программные, физические, организационные и другие) должны использоваться одновременно и под централизованным контролем конечно этого можно достичь. Это будет во многом способствовать развитию предприятия. Мы снова надо подчеркнуть, что сегодня большое внимание уделяется информационной безопасности мы должны

дать. Потому что регулирование информационных потоков сегодня актуально остается одной из проблем.

ИСПОЛЬЗОВАНИЕ ЛИТЕРАТУРА:

1. Ганиев С.К., Каримов М.М., Ташев К. А. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В Ташкенте 2007 год.

2. С.С. Касимов Учебное пособие по информационным технологиям Ташкент 2007г.

3. Ганиев С.К., Каримов М.М. Информационная безопасность в вычислительных системах и сетях Ташкент 2003 г.