"Raqamli iqtisodiyot va axborot texnologiyalari" elektron ilmiy jurnali
№ 2(2), aprel-iyun, 2021 yil

ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

ХАШИМХОДЖАЕВ Шарафутдин Ишанходжаевич
Доцент кафедры «Цифровая экономика и информационные технологии» Ташкентского государственного экономического университета, к.э.н.

Аннотация: *В статье показано, что в условиях формирования цифровой экономики обеспечение информационной безопасности является одним из важнейших условий стабильного функционирования современных информационных систем. Кроме того, отмечено, что для эффективной организации информационной безопасности большое значение в современный период играют программные комплексы, способствующие оптимизации функционирования информационных систем экономических субъектов хозяйствования.*

Ключевые слова: *информационные системы, информационная безопасность, цифровая экономика, угрозы безопасности, эффективность, информационный обмен.*

Аннотация: *Мақолада кўрсатилишича, рақамли иқтисодиёт шаклланаётган шароитда ахборот хавфсизлигини таъминлаш замонавий ахборот тизимларининг барқарор ишлашининг муҳим шартларидан бири ҳисобланади. Бундан ташқари, ахборот хавфсизлигини самарали ташкил этишда хўжалик юритувчи субъектларнинг ахборот тизимлари фаолиятини оптималлаштиришга хизмат қилувчи дастурий таъминот тизимлари замонавий даврда катта аҳамият касб этиши таъкидланган.*

Калит сўзлар: *ахборот тизимлари, ахборот хавфсизлиги, рақамли иқтисодиёт, хавфсизлик таҳдидлари, самарадорлик, ахборот алмашинуви.*

Общемировые процессы информационной глобализации диктуют не только необходимость повсеместного внедрения ИКТ в экономике и сферах жизни стран, но и условия обеспечения безопасности информационных систем. Узбекистан одним из первых в Центральной Азии присоединился к международной системе безопасности в сфере информационных и коммуникационных технологий.

Исследования ученых показывают, что экономическая безопасность представляет собой комплексное понятие, которое включает в себя политическую безопасность, финансовую, социальную, инновационную и в том числе информационную.

Сегодня доля цифровой экономики в ВВП страны составляет 2,2 процента. К 2023 году планируется ее увеличить в два раза, а долю электронных госуслуг довести к 2022-му до 60 процентов.

Узбекистан уверенно вошел в век цифровизации, о чем свидетельствуют поэтапные действия правительства направленные на увеличение скорости и качества Интернета, повсеместного внедрения информационно-коммуникационных технологий во все сферы жизнедеятельности страны.

При этом, особое внимание уделяется вопросам обеспечения информационной безопасности, решению ряда задач по обеспечению зашиты от потенциальных кибератак, бесперебойного функционирования объектов информатизации и информационной инфраструктуры Республики Узбекистан.

В этих целях проводится мониторинг событий, предотвращение и реагирование на угрозы и инциденты кибербезопасности в национальном сегменте сети Интернет.

Вопросы обеспечения безопасности в информационном пространстве Uznet приобретают сегодня особое значение.

В течении 2020 года было выявлено более 27000000 событий вредоносной и подозрительной сетевой активности, исходящей из адресного пространства национального сегмента сети Интернет, которые в свою очередь представляли угрозы безопасному и стабильному функционированию информационных систем и ресурсов государственных органов и других организаций.

Как показывает современная действительность, при функционировании современных информационных систем с целью защиты информации используются правовые, организационные и технические меры, которые направленны на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации, соблюдение конфиденциальности информации ограниченного доступа, реализацию права на доступ к информации [1].

Выбор способов и средств защиты зависит от поставленных задач по обеспечению безопасности:

- ограничение доступа;
- разграничение полномочий;
- обеспечение доверия;
- защита содержания.

Самый распространенный способ ограничения доступа к ресурсам – это создание учетных записей с помощью встроенных средств информационной системы. Отличаются только протоколы, применяемые при передаче данных идентификации пользователя, начиная от кодирования и вплоть до использования значений хеш-функций и шифрования, выбор протокола определяет уровень безопасности доступа. Независимо от протокола учетные записи могут обеспечить лишь грубое деление пользователей на доверенных и недостоверных, если же мы хотим предоставлять пользователям разные полномочия, то для этого нужны другие решения.

Обычно в организациях используются общие электронные документы, подготовленные в головном подразделении, которые обычно содержат таблицы с данными, используемыми сотрудниками подчиненных подразделений. Искажение данных может привести к нарушению сводной отчетности организации. Для разграничения полномочий по работе с данными в электронных документах задействованы встроенные возможности редакторов, определив группы пользователей, которым будет предоставлено право на чтение или на внесение изменений в электронный документ или только в определенные листы и области. Такой способ разграничения полномочий предоставляет больше возможностей, чем простое «пустить – не пустить», но в целом возможности редакторов ограничены и помимо ограничения редактирования, других задач решать они не могут [2].

Намного большими возможностями по разграничению полномочий пользователей при работе с электронными документами обладают специализированные программные средства, например, такие, как служба управления правами ActiveDirectory. С ее помощью можно разграничить права на чтение, редактирование, копирование, печать и пересылку электронных документов. С помощью этой службы можно применять единую корпоративную политику по использованию и распространению конфиденциальных сведений. Заданная для электронного документа политика остается с ним независимо от его перемещения, отправки

или пересылки. Для защиты содержания электронных документов и заданных политик используется шифрование с помощью встроенных средств операционной системы Microsoft.

Существующие способы разграничения доступа позволяют защитить электронные документы от неправомерного доступа, уничтожения, модифицирования, копирования и распространения в рамках одной системы, но не могут обеспечить решение вопроса доверия при электронном взаимодействии пользователей разных систем. Использование полноценного электронного документооборота предполагает обеспечение доверия к самим электронным документам независимо от того, где и кем они созданы.

Наиболее успешно вопрос доверия решается с помощью так называемой электронной подписи. Простая электронная подпись позволяет определить создателя подписи путем добавления к электронному документу подтверждающего значения, такого как код, строка, личная подпись или отпечаток пальца, полученные с помощью считывателя. Такие способы широко распространены, не требуют больших затрат, просты в использовании, чем, собственно, и привлекательны для пользователей.

Уровень безопасности, который обеспечивает простая электронная подпись, невысок, но может быть вполне достаточен, например, для обеспечения доверия во внутреннем документообороте. Многие платежные системы для обеспечения доверия при электронном взаимодействии с клиентами используют простую электронную подпись [3].

Более высокий уровень безопасности обеспечивает усиленная электронная подпись, которая представляет собой набор данных вместе с зашифрованной частью, позволяющей однозначно установить создателя электронной подписи и проверить целостность электронного документа. Шифрование выполняется с использованием личного ключа пользователя и предполагает применение средств криптографической защиты информации, что требует определенных затрат на их приобретение, установку и настройку, а также на предварительное обучение пользователей работе с такими средствами.

Существуют и простые решения, когда средства криптографической защиты информации устанавливаются на удаленном сервере и туда предоставляется доступ доверенным пользователям. При проверке электронной подписи выполняется расшифровывание зашифрованной части подписи с помощью известного открытого ключа пользователя, который хранится вместе с учетной записью пользователя. Если же пользователи взаимодействуют, не используя общее хранилище учетных данных, то для обеспечения доверия к открытому ключу применяется документ, подтверждающий владение пользователя открытым ключом, который носит название сертификата открытого ключа или ключа проверки электронной подписи. Создают сертификаты удостоверяющие центры, которым должны доверять все участвующие в электронном взаимодействии пользователи. Доверие к сертификату обеспечивает электронная подпись, созданная удостоверяющим центром [4].

Очень важная задача при электронном взаимодействии – это соблюдение конфиденциальности информации ограниченного доступа с помощью защиты содержания электронных документов. Есть разные решения этой задачи, выбор зависит от способа взаимодействия пользователей [5].

При сетевом взаимодействии пользователей можно ограничить доступ к передаваемым данным, используя набор протоколов IPSecurity. Для защиты данных и ограничения доступа используется шифрование на общем ключе, при этом могут применяться разные криптографические алгоритмы и программные средства.

Если пользователи взаимодействуют посредством почтовых сообщений, то для их защиты создан стандарт протоколов S/MIME. Защита передаваемых почтовых сообщений обеспечивается в этом случае совместным использованием электронной подписи и

шифрования. Здесь все участники взаимодействия должны получить свой сертификат в удостоверяющем центре с необходимыми указаниями о назначении ключей [6].

Существующие информационные и платежные системы используют совокупность решений для защиты передаваемых электронных данных и обеспечения доверия к ним, но есть и немало схем, где используется только одно из вышеперечисленных решений.

При удаленном взаимодействии пользователей разных систем наиболее эффективными являются решения с использованием сертификатов, обеспечивающие доверие ко всем взаимодействующим сторонам и позволяющие удаленно согласовать ключи шифрования для защиты передаваемых электронных данных, а также использовать в рамках электронного документооборота усиленную электронную подпись. Этим достигается наиболее высокий уровень защищенности передаваемых электронных документов и степени доверия к ним.

На сегодняшний день для эффективной организации информационной безопасности в информационных системах внедряется комплексная система безопасности на основе программного продукта SECURE TOWER, который позволяет обеспечить:

- защиту от преднамеренного хищения или случайной утечки данных;
- управление операционными, репутационными и правовыми рисками;
- ведение архива бизнес-коммуникаций организации;
- расследование инцидентов в ретроспективе.

Совмещение разных способов контроля информации (лингвистического, статистического, атрибутивного, цифровых отпечатков и т.д.) и возможность создания многокомпонентных политик безопасности позволяет повысить эффективность работы службы информационной безопасности [7].

Как показывает практика, недостаточно только обнаружить инцидент, важно оперативно на него отреагировать. В случае обнаружения инцидента, ответственному сотруднику службы информационной безопасности будет незамедлительно электронное письмо с уведомлением об инциденте и его описании.

Управление операционными рисками с помощью SecureTower осуществляется путём выявления случаев нецелевого использования персоналом рабочего времени и корпоративных ресурсов [8].

Благодаря своему инструментарию SecureTower дает возможность минимизировать вероятность возникновения операционных рисков и позволяет оптимизировать бизнес-процессы компании.

Программа создает своеобразный архив для ведения «истории» внутрикорпоративных бизнес-процессов и событий.

Это позволяет расследовать любой случай утечки конфиденциальной информации в ретроспективе. Обратившись к определенному сообщению, можно посмотреть всю историю коммуникации абонентов [9].

SecureTower обеспечивает полный контроль мобильных рабочих станций и переносных компьютеров, покидающих пределы сети компании.

Ещё одной опцией программного продукта является возможность централизованной настройки и управления системой в территориально распределенных офисах.

SecureTower централизованно устанавливается и настраивается из одной консоли и не требует изменения инфраструктуры сети или покупки дополнительного дорогостоящего оборудования.

Таким образом, можно сделать вывод, что информационная безопасность является важным компонентом экономической безопасности и фактором оптимизации деятельности предприятия в условиях комплексного информационного обмена.

Список литературы

1. Барт А.А. Подходы к обеспечению экономической безопасности России в долгосрочной перспективе // А.А. Барт, Л.В. Барт // Современные процессы в развивающейся экономике: сборник научных трудов – Ульяновск: УлГТУ, 2011.

2. Бегалов Б.А., Жуковская И.Е. Методические основы влияния информационно-коммуникационных технологий на развитие национальной экономики. Монография. Т.: Иктисодиет. 2018. – 178 с.

3. Горбашко Е.А. Влияние цифровизации на качество жизни с позиций устойчивого экономического развития // Сборник статей по итогам XIV международной научно-практической конференции «Современный менеджмент: проблемы и перспективы». СПб.: Изд-во СПбГЭУ, 2019 г., с. 29.

4. Жуковская И.Е. Совершенствование методологии применения информационно-коммуникационных технологий в статистической деятельности в условиях формирования цифровой экономики. Монография. Ташкент: Инновацион ривожланиш нашриёт-матбаа уйи. 2020, 160 с.

5. Прохорова М.П. Теория принятия решений в менеджменте: учебное пособие / Прохорова М.П. Нижний Новгород: ВГИПУ, 2017. - 71 с.

6. Хашимходжаев Ш.И. Влияние цифровой трансформации на экономические процессы в Республике Узбекистан. Сборник статей по итогам XIV международной научно-практической конференции «Современный менеджмент: проблемы и перспективы». Изд-во Санкт Петербургского государственного экономического университета. 2019, С. 505-509.

7. Юрков А.В. Укрупненная классификация систем поддержки принятия решений // Прикладная информатика 2018 № 3. Часть 2., с.157.

8. www.abt.ru - сайт автоматизации документооборота для бизнеса.

9. infocom.uz - интернет-издание infoCOM.UZ - Информационно-коммуникационные технологии Узбекистана.