Қазақстан Республикасы Тәуелсіздігінің 30 жылдығына арналған «Сейфуллин оқулары – 17: «Қазіргі аграрлық ғылым: цифрлық трансформация» атты халықаралық ғылыми – тәжірибелік конференцияға материалдар = Материалы международной научно – теоретической конференции «Сейфуллинские чтения – 17: «Современная аграрная наука: цифровая трансформация», посвященной 30 – летию Независимости Республики Казахстан.- 2021.- Т.1, Ч.1 - С.8-10

ЗАЩИТЫ ИНФОРМАЦИЙ НА ПРЕДПРИЯТИЯХ СЕЛЬСКОХОЗЯЙСТВЕННОГО ПРОИЗВОДСТВА

Сейткулов Е.Н.,
Есхожин Д.К, магистрант
ЕНУ им. Л.Гумилева, г.Нур-Султан

В настоящее время информационные системы (ИС) различного масштаба стали неотъемлемой частью базовой инфраструктуры государства, бизнеса, гражданского общества и производственной сферы. Все больше защищаемой информации переносится в ИС. Современные информационные технологии не только обеспечивают новые возможности организации бизнеса, ведения государственной и общественной деятельности, но и создают значительные потребности в обеспечении безопасности для защиты информации.

Защита информация – серьезная проблема и реальная угроза для большинства предприятий, представляющих различные отрасли в том числе и с\х предприятий. Данные могут быть утеряны по причине злого умысла третьих лиц, по неосторожности сотрудников. При умышленной организации наносится серьезный ущерб. В условиях конкуренции такой прием используют многие сторонние организации, чтобы получить преимущество над конкурентами, пусть и таким незаконным способом.

Чтобы исключить неблагоприятные последствия утраты данных, нужно использовать системы защиты информационных активов. Их создание должно быть на высоком профессиональном уровне, с применением современных технических и программных средств.

Основными процедурами регистрации пользователей в ИС являются процедура идентификации — получение ответа на вопрос «Кто Вы?» и аутентификации — доказательства того, что «Вы именно тот, кем представляетесь». Несанкционированное получение злоумышленником доступа к ИС связано, в первую очередь, с нарушением процедуры аутентификации.

Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов.

Идентификация и аутентификация — это первая линия обороны, «проходная» информационного пространства организации.

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает.

В любом случае функция вычисления эталона из аутентификационной информации должна быть однонаправленной, т. е. легко рассчитываться, но представлять собой вычислительную проблему при попытке вычисления в обратном направлении.

Надежная идентификация и затруднена не только из-за сетевых угроз, но и по целому ряду причин. Во-первых, почти все аутентификационные сущности можно узнать, украсть или подделать. Во-вторых, имеется противоречие между надежностью аутентификации, с одной стороны, и удобствами пользователя и системного администратора с другой. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить аутентификационную информацию (ведь на его место мог сесть другой человек), а это не только хлопотно, но и повышает вероятность того, что кто-то может подсмотреть за вводом данных. В-третьих, чем надежнее средство защиты, тем оно дороже.

Современные средства идентификации/аутентификации должны поддерживать концепцию единого входа в сеть. Единый вход в сеть — это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная идентификация/аутентификация становится слишком обременительной. К сожалению, пока нельзя сказать, что единый вход в сеть стал нормой, доминирующие решения пока не сформировались.

В отличие от некоторых весьма вольных трактовок, будем следовать строгим определениям, данным в работах [1,2,3]. Среди широко применяемых в последние 3–5 лет терминов описания процесса идентификации/аутентификации введено понятие индивидуальных характеристик, доказывающих подлинность субъектов или факторов. К факторам идентификации/аутентификации относят:

- владение скрытой для посторонних информацией (запоминаемая либо хранящаяся конфиденциальная информация). Примерами могут служить пароль, персональный идентификационный код (PIN), секретные ключи и т.п.;
- обладание материальным носителем информации (карта с магнитной полосой, электронные ключи классов touch memory и eToken, смарт-карта, дискета и т.д.);
- биометрические характеристики субъекта (отпечатки пальцев, голос, геометрия лица, особенности сетчатки и радужной оболочки глаз и т.п.).

В зависимости от используемых в технологиях идентификации и аутентификации факторов (ИАФ) различают однофакторную или двухфакторную аутентификацию. Понятие трехфакторной аутентификации в последнее время используется достаточно редко ввиду призрачности ее промышленного применения при современном состоянии технических средств. Рассмотрим наиболее развитые методы идентификации и аутентификации с точки зрения применяемых в них технологий.

В последнее десятилетие интенсивно развивается направление электронной идентификации, в которой сбор информации происходит с минимальным участием человека. Это объясняется тем, что оператор может допустить ошибку при вводе данных, например с клавиатуры компьютера. Ведь на поиск и исправление ошибок в больших массивах данных может уйти слишком много времени. Главное в системе автоматизации – достоверность информации. Технологии автоматической идентификации наиболее полно соответствуют требованиям компьютерных систем и систем управления, где нужно четко распознавать объекты в реальном масштабе времени.

Для того чтобы понять, что такое аутентификация, обратимся к простому примеру: ваш сотовый телефон. Телефон – это устройство, куда для начала работы вы вкладываете свою SIM-карту. Когда вы включаете телефон, на дисплее появляется надпись: "Введите PIN-код". После правильного ввода PIN-кода (как правило, это четыре легко запоминаемые цифры) и кратковременной задержки телефон начинает работать. Налицо так называемая двухфакторная аутентификация. Вам надо иметь персональный носитель (SIM-карту) и знать личный PIN-код. Они связаны между собой. Причем эта связь закладывается администратором оператора сотовой связи при предпродажной подготовке контрактов с определенным тарифом и самих SIM-карт. Сам телефонный аппарат по аналогии с корпоративными информационными системами играет роль компьютера. Аналогом SIM-карты может являться микропроцессорная смарт-карта или устройство eToken, к которому привязан личный PIN-код. Только в отличие от сотового телефона PIN-код для доступа к информационной системе предприятия содержит, как правило, не менее 5 – 7 символов различных регистров (не только цифр). Да и алгоритмы аутентификации и шифрования там намного сложнее, чем традиционные A3 (алгоритм аутентификации), A8 (алгоритм генерации криптоключа), A5/2 (собственно алгоритм шифрования оцифрованной речи для обеспечения конфиденциальности переговоров), используемые в сотовой связи.

Список литературы

1. Курило А.П. и др. Обеспечение информационной безопасности бизнеса. –М.: БДЦ-пресс, 2005.

2. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети – анализ технологий и синтез решений — М., ДМК Пресс, 2004.

3. Сарбуков А., Грушо А. Аутентификация в компьютерных системах//Системы безопасности. – 2003. – №5 (53).