УДК 004.514.6

ОСНОВЫ ФОРМИРОВАНИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИЯХ ТЕКСТИЛЬНОЙ ПРОМЫШЛЕННОСТИ

BASES OF FORMATION OF THE INFORMATION SECURITY SYSTEM AT TEXTILE INDUSTRY ENTERPRISES

И.Г. ЛУКМАНОВА, Р.С. ГОЛОВ, В.Ю. ТЕПЛЫШЕВ, В.Г. СМИРНОВ

I.G. LUKMANOVA, R.S. GOLOV, V.YU. TEPLYSHEV, V.G. SMIRNOV

(Национальный исследовательский Московский государственный строительный университет, Московский авиационный институт (национальный исследовательский университет))

(Moscow State University of Civil Engineering (National Research University, Moscow Aviation Institute (National Research University))

E-mail: lukmanova@mgsu.ru; roman_golov@rambler.ru; teplyshev@tbnenergo.com; svgvgy@mail.ru

Исследование посвящено проблеме формирования системы информационной безопасности предприятия текстильной промышленности. Авторами определяются предпосылки к ее созданию в рамках программно-технического комплекса текстильного предприятия в условиях цифровизации его экономических и технологических процессов. Определяются ключевые принципы построения системы информационной безопасности. На основе этих принципов формируется структура данной системы с учетом конкретных угроз и методов противодействия им, на основе которой исследуются различные методы и технологии программной и аппаратной защиты данных текстильного предприятия.

The study is devoted to the problem of forming the information security system of a textile enterprise. The authors determine the prerequisites for its creation within the program and technical complex of a textile enterprise in the conditions of digitalization of its economic and technological processes. The key principles of building an information security system are defined. Based on these principles, the structure of this system is formed taking into account specific threats and methods of counteraction against them, on the basis of which various methods and technologies of software and hardware protection of data of a textile enterprise are explored.

Ключевые слова: информационная безопасность, программно-технический комплекс, защита данных, аппаратные и программные средства защиты, пакеты прикладных программ, структура системы защиты данных.

Keywords: information security, software and hardware complex, data protection, hardware and software protection tools, application software packages, data protection system structure.

В современных экономических условиях одним из важнейших элементов инфраструктуры практически каждого предприятия текстильной промышленности выступает его программно-технический комплекс (ПТК), включающий в себя аппаратную и программную составляющие. В состав его аппаратной части входят компьютеры, сервера, контроллеры и исполнительные механизмы, локальная сеть и действующее в ее

рамках коммуникационное оборудование. Они обеспечивают непрерывный обмен информацией между отдельными подсистемами предприятия, сбор данных об их функционировании, а также возможность централизованного управления текстильным производством. Не менее важная программная составляющая включает в себя операционные системы, ERP-систему, специализированные пакеты прикладных программ (ППП), применяемые предприятием для управления технологическими процессами производства, бухгалтерское программное обеспечение и т.д. С позиции теории систем программно-технический комплекс можно рассматривать в виде совокупности локальных ПТК (ЛК). Органично интегрированные между собой, программная и аппаратная части ПТК представляют собой единую систему управления предприятием текстильной промышленности, в рамках которой осуществляется весь цикл управления производством.

Все более возрастающая роль и важность ПТК как ключевой системы управления предприятием порождает новые достаточно специфические риски, связанные с его информационной безопасностью. Цифровизация производственных, экономических и административно-управленческих процессов приводит к тому, что, с одной стороны, ПТК обеспечивает стабильность функционирования производства, а с другой – во входящих в его состав базах данных и ППП хранится стратегически важная конфиденциальная информация о его экономических показателях, используемых при производстве технологиях, принципах организации производства и подобные данные. Хищение этих данных, либо намеренная организация технических сбоев в ПКТ способны нанести предприятию серьезный экономический урон, что обусловливает важность обеспечения информационной безопасности предприятия, в основе которой должен лежать системный комплекс методов и технологий, защищающих программно-технический комплекс на всех уровнях его иерархии. Разработке прикладных основ информационной безопасности предприятия текстильной промышленности и посвящено данное исследование.

При построении системы информационной безопасности, охватывающей все задачи, решаемые на предприятии, рекомендуется использовать нижеперечисленные принципы.

1. *Построение системы безопасности* от несанкционированного доступа (НСД) с наименьшими затратами и с большим эффектом.

2. *Масштабируемость:* программное обеспечение должно работать с приемлемой, не сильно сниженной производительностью, без внесения в него существенных изменений при увеличении мощности и количества используемого оборудования.

3. *Многозвенность:* каждый архитектурный уровень ПТК (web-сервер, сервер приложений, сервер баз данных) реализует функции, наиболее ему присущие. В каждом звене должен работать встроенный компонент защиты и аутентификации информации.

4. *Иерархичность функционирования* ПТК предусматривает реализацию защиты информации на всех иерархических уровнях предприятия.

5. *Обеспечение отказоустойчивости и надежности.*

Перечисленные принципы и базирующиеся на них методы позволяют построить структурную схему элементов защиты ПТК на предприятии.

ЛК, обеспечивающий безопасность информации от НСД, составляет комплекс с другими ЛК и решает в автоматизированном режиме ситуационные задачи защиты от НСД, определяет уровень безопасности в меняющихся условиях.

Различные предприятия могут иметь разнообразную топологию средств защиты информации для обеспечения защищенного режима взаимодействия с внешними системами. Своевременная передача информации без искажений, перехвата, в нужное место является актуальной задачей. Структурная схема элементов защиты ПТК представлена на рис. 1.

В состав структурной схемы элементов защиты ПТК предприятия текстильной промышленности входят 4 блока.

Блок 1 – Паспорт нарушителя. Позволяет определить, кто или что является причиной отказа в информационной системе. Наравне с проникновением в систему преступ-

ника, отказы могут происходить из-за низкого уровня качества оборудования или недобросовестного администрирования комплекса программных средств в составе ПТК. Если причина – удавшаяся атака, тогда выявляются нарушение и нарушитель. Таковым может быть свой сотрудник или посторонний хакер (действующий извне).

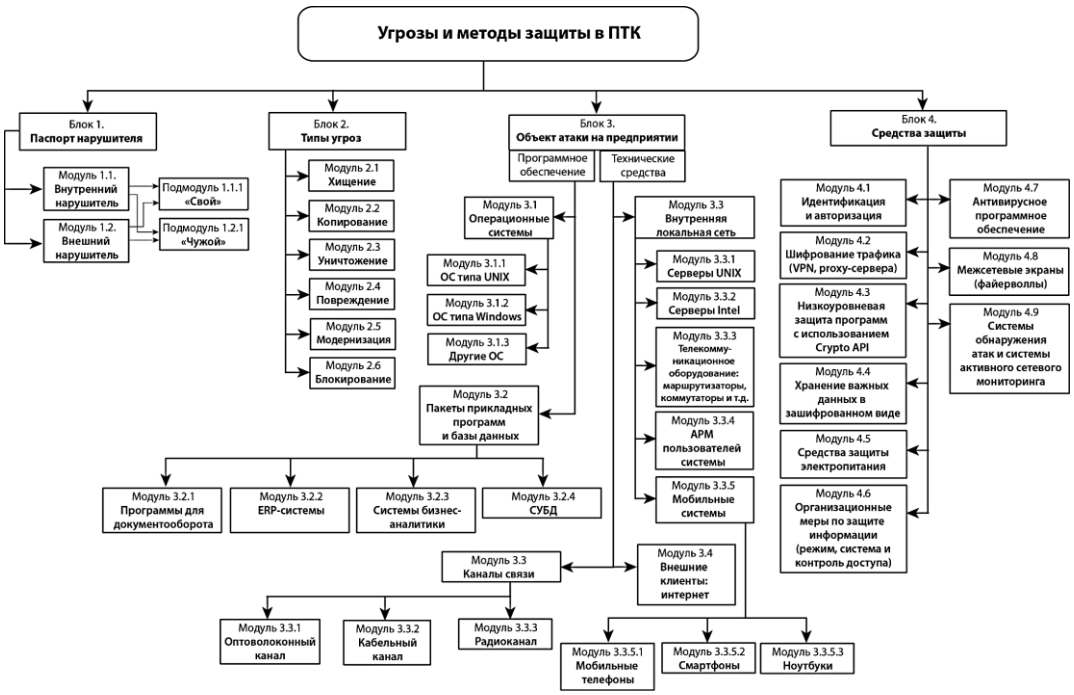

Рис. 1

Блок 2 – Тип угроз. Анализирует типы угроз, которые могут определяться: как хищение, копирование, уничтожение, повреждение, блокирование. Злоумышленник использует средства, направленные на объект атаки и отвечающие его цели: программно-аппаратные или программные средства – аппаратные закладки (непосредственно включающиеся в канал передачи информации или перехватывающие различные побочные электромагнитные излучения), вирусы, троянские программы, программные модули, реализующие уязвимости операционных систем и сетевых протоколов.

Блок 3 – Объект атаки. Позволяет определить объект атаки в ПТК на предприятии. Учитывая, что ПТК состоит из двух взаимосвязанных частей – комплекса обеспечения и комплекса технических средств, то именно они и могут быть разноаспектными объектами угроз.

Из комплекса программного обеспечения в качестве объектов атак можно выделить операционные системы (ОС), пакеты прикладных систем и системы управления базами данных (СУБД). Угроза может быть фиксирована в определенном месте ПТК – на конкретном электронном устройстве. Это позволяет в дальнейшем ставить датчики в конкретные места ПТК для определения уровня защиты.

Нападению могут подвергаться серверы, рабочие станции, мобильные компьютеры, смартфоны, планшеты, имеющие подключение к Интернету.

Угрозы информационной безопасности ПТК могут быть реализованы при использовании как морально устаревших проводных (витая пара и пр.), более современных оптоволоконных, так и радио- (Wi-Fi, Bluetooth и пр.) каналов связи. Очевидно, что в условиях интеграции ПТК с сетью Интернет, отказаться от которой в современных условиях невозможно, ограничиваться лишь физической защитой канала связи неразумно.

Телекоммуникационному оборудованию, к которому относятся коммутаторы, маршрутизаторы и другие устройства, необходима дополнительная защита. Использование специальных программно-аппаратных бранд-

мауэров (firewall) типа Cisco PIX (IOS) (см. подробнее блок 4) позволяет защитить все сегменты ПТК.

Блок 4 – Средства защиты. Определяет на основе анализа блоков 1...3 оптимальные средства защиты информации. В ПТК на различных иерархических уровнях предприятия могут быть использованы следующие способы: антивирусные программы; межсетевые экраны в виде программно-аппаратных и программных средств защиты; средства идентификации и аутентификации пользователей с использованием клавиатуры, USB-хранилищ и других ключевых носителей, а также биометрических технологий; различные криптографические технологии, такие как VPN и инфраструктура открытых ключей (PKI) в целом; программная и программно-аппаратная защита на прикладном уровне (использование при разработке приложений Crypto API); система противодействия техническим средствам снятия информации (генераторы шума, эффективное экранирование выделенных помещений и каналов передачи информации); административные меры по защите информации (организация системы контроля доступа в определенные помещения и режима информационной безопасности на предприятии в целом).

Антивирусные программы позволяют с известной степенью вероятности нейтрализовать воздействие различных вредоносных программ (прежде всего вирусов и "троянцев"), удалять известные и блокировать неизвестные вирусы. *В современных условиях функционирование ПТК без антивирусных средств защиты практически невозможно.*

При входе пользователя в информационную систему используются средства идентификации и аутентификации. Идентификация позволяет сравнить заранее сохраненный идентификатор с вводимым при доступе к системе. Аутентификация подтверждает принадлежность идентификатора субъекту, то есть устанавливает аутентичность пользователя.

Наиболее эффективным способом идентификации являются одноразовые пароли (аутентификация при помощи защищенных носителей – смарт-карт, USB-ключей), для применения которых необходимо внедрение современных протоколов аутентификации, использующих технологии инфраструктуры открытых ключей, например, Kerberos 5.

Максимальную защищенность от атак изнутри обеспечивают терминальные серверы и тонкие клиенты, или терминалы для автоматизации рабочих мест пользователя (адекватная замена персональным компьютерам). На сегодняшний день серверные операционные системы ведущих мировых производителей (Microsoft, Sun Microsystems, Red Hat Linux и др.) поддерживают такой режим работы.

Практика построения информационных порталов показала, что для их эффективного функционирования необходимо использовать уровень серверов приложений, предоставляющих всем пользователям единый интерфейс. Это позволяет не загружать клиентскую часть и решает проблему кросс-платформенной совместимости в случае использования, например, web-технологий и технологии Java.

При работе в ПТК с различными приложениями – пакетами прикладных программ (ППП) – необходимо решать задачу обеспечения конфиденциальности данных в самих приложениях. Защищенное взаимодействие между различными ППП на прикладном уровне может быть обеспечено на стадии их разработки путем использования различных криптографических API, которые уже на протяжении нескольких лет являются неотъемлемыми компонентами различных средств разработки программного обеспечения.

В последнее время широкую популярность получило использование в ПТК инфраструктуры открытых ключей. Развертывание на предприятии системы удостоверяющих центров значительно (практически до нуля) снижает риск хищения и модифицирования конфиденциальной информации.

На российском рынке лидерами в этой области являются продукты фирмы КриптоПро для ОС Windows или Keon CA фирмы RSA Security (реализация которого существует практически для всех серверных операционных систем), имеющие сертификаты Гостехкомиссии России.

Идеология защиты ППП системы электронного документооборота, например, Documentum 5, строится на технологии удостоверяющих центров на базе открытых ключей (PKI). Удостоверяющие центры позволяют использовать электронно-цифровую подпись (ЭЦП) и тем самым обеспечить невозможность отрицания автора документа от причастности к его созданию, а также при необходимости обеспечить криптографическую защиту передаваемого по различным сетям документа, обеспечивая конфиденциальность содержащейся в нем информации.

Используемые в ПТК функционально-ориентированных информационных систем (ERP – системы для учета финансово-хозяйственной деятельности, CRM – системы управления взаимоотношениями с клиентами и др.), а также системы управления базами данных должны обладать системой защиты (прежде всего идентификации и аутентификации) на своем прикладном уровне. При этом эффективность использования таких систем возрастает в случае поддержки с их стороны LDAP-подобных служб каталогов (де-факто являющихся на сегодня стандартом), что позволяет интегрировать данные системы в сетевую среду ПТК с минимальными затратами и без ущерба для информационной безопасности.

Иногда для защиты конфиденциальной информации недостаточно разграничить доступ для пользователя к ресурсам на уровне операционных систем. Усилить защиту можно применением "сейф-контейнеров", разработанных, например, российской фирмой Алладин Р.Д.

Эта технология заключается в том, что зашифрованная информация записывается в "сейф-контейнер" (специально выделенное защищенное пространство на жестком диске или другом информационном носителе). Используется ключ eToken для USB-порта, обеспечивающий прозрачный для пользователя процесс шифрования/дешифрования информации.

На разных иерархических уровнях ПТК должен функционировать в режиме защиты от сбоев по электропитанию. Надежность питания обеспечивают источники бесперебойного питания (ИБП), например, фирмы APC (российского подразделения французской компании Schneider Electric), которые в зависимости от нагрузки, на которую рассчитаны, могут быть и компактными, и размером с компьютерную стойку-шкаф.

Если в ПТК происходит сбой электропитания, ИБП начинает поддерживать работоспособность системы в автономном режиме. Если в течение номинального срока электропитание не возобновляется, специальное программное обеспечение, например, PowerChute, активизируется и в автоматическом режиме корректно закрывает открытые приложения, сводя неудобства по сбою электропитания к минимуму. Потеря информации при этом практически исключена.

Для защиты информации полезны и организационно-административные меры:

- каждому пользователю предписывается иметь свой пароль, разграничивающий доступ и, возможно, с течением времени заменяемый;
- при допуске к работе каждый пользователь проходит проверку на пригодность работы на оборудовании и с конфиденциальной информацией;
- каждый пользователь должен иметь доступ к ограниченному списку помещений, определяемым его полномочиями.

На рынке средств защиты информации относительно недавно появились системы активного мониторинга (CAM) и системы обнаружения атак (СОА). Первые предназначены для жесткого контроля за действиями пользователей и происходящих процессов на серверах и рабочих станциях. Клиентские агенты данной системы отслеживают пользователей и запущенных ими в системе процессов, а также анализируют состояние журналов операционной системы. В случае обнаружения несанкционированных действий работа системы блокируется, а сообщение с подробным докладом отсылается на специальный сервер.

Второй класс систем предназначен для диагностики сетевых правонарушений. На наиболее важных участках сети устанавливаются сетевые датчики (серверы), которые анализируют все проходящие через них пакеты на предмет выявления сигнатур атак,

блокируют трафик со скомпрометированных узлов и на сервер системы сообщение с отчетом и перехваченными пакетами. Возможна также установка агентов СОА непосредственно на критически важные серверы, которые анализируют весь входящий на сервер трафик и генерируют сообщения об обнаруженных попытках атак.

Вышеперечисленные средства защиты и анализ угроз позволяют сформировать модель защиты ПТК, работающего в условиях интеграции с сетью Интернет.

Среди прочих выделяются хакерские атаки, направленные на достижение отказа в обслуживании (DoS – Denial of Service). Они несут опасность блокирования информации, и информационные ресурсы становятся недоступными пользователям. Самой эффективной разновидностью таких атак являются атаки распределенного отказа в обслуживании (DDoS – Distributed DoS). Источниками атаки являются тысячи или даже миллионы сетевых хостов (как правило, зараженных специально разработанным вирусом) по всему миру.

Руководство предприятия вольно выбрать эффективные средства защиты ПТК на разных иерархических уровнях в различных сетях. Стратегия политики безопасности определяет множество решений типа firewall, систем обнаружения вторжения и механизмов контроля доступа. При выборе средств защиты от НСД могут использоваться различные эвристические подходы, обеспечивающие выбор правильных направлений в его реализации. Детальный анализ возможностей защиты позволяет остановиться на тех или иных средствах, применяемых при определенных условиях.

Как правило, управление информационной безопасностью ПТК осуществляется на основе мониторинга его состояния с консоли системного администратора, проводящего анализ потенциальных и реальных угроз, на основе чего определяется политика безопасности на предприятии текстильной промышленности. При этом, если средства защиты выведены из строя, эксплуатировать ПТК без введения резервных средств защиты нельзя. При изменении ситуации может изменяться и комплекс средств защиты, их состав, предпочтительность использования одних перед другими. Для эффективной защиты информации в компьютерных системах используется сочетание нескольких видов защит. Например, антивирусные программы эффективны в комплексе с программно-аппаратными брандмауэрами.

ВЫВОДЫ

Выбор средств защиты всегда определяется заказчиком. По мнению авторов, основополагающим критерием в данном вопросе является их соответствие уровню угроз. Самостоятельная разработка средств защиты информации требует огромных трудовых и финансовых ресурсов (если, конечно, учитывается эффективность разрабатываемой системы). Поэтому, на наш взгляд, наиболее эффективным путем создания системы защиты информации в ПТК является интеграция лучших продуктов ведущих мировых производителей (возможно, совместно с собственными разработанными средствами).

ЛИТЕРАТУРА

1. *Голов Р.С., Мыльник А.В.* Инновационно-синергетическое развитие промышленных организаций (теория и методология). – М.: ИТК "Дашков и К°", 2018.

2. *Трайнев В.А., Теплышев В.Ю., Трайнев И.В.* Новые информационные коммуникационные технологии в образовании. – М.: ИТК "Дашков и К°", 2009.

3. *Евдокимова Л.И.* Современные проблемы позиционирования текстильной промышленности в экономике России // Аграрный вестник Урала. – 201, № 3. С. 93...95.

4. *Назарова М.В.* Автоматизация проектирования тканей по заданным параметрам // Изв. вузов. Технология текстильной промышленности. – 2008, № 2. С. 138...140.

5. *Писарская О.В.* Технологии неоиндустриализации экономики: кластеризация в химической и текстильной промышленности // Экономика: вчера, сегодня, завтра. – 2017, № 7. С. 196...204.

REFERENCES

1. Golov R.S., Myl'nik A.V. Innovatsionno-sinergeticheskoe razvitie promyshlennykh organizatsiy (teoriya i metodologiya). – M.: ITK "Dashkov i Ko", 2018.

2. Traynev V.A., Teplyshev V.Yu., Traynev I.V. Novye informatsionnye kommunikatsionnye tekhnologii v obrazovanii. – M.: ITK "Dashkov i Ko", 2009.

3. Evdokimova L.I. Sovremennye problemy pozitsionirovaniya tekstil'noy promyshlennosti v ekonomike Rossii // Agrarnyy vestnik Urala. – 201, № 3. S. 93...95.

4. Nazarova M.V. Avtomatizatsiya proektirovaniya tkaney po zadannym parametram // Izv. vuzov. Tekhnologiya tekstil'noy promyshlennosti. – 2008, № 2. S. 138...140.

5. Pisarskaya O.V. Tekhnologii neoindustrializatsii ekonomiki: klasterizatsiya v khimicheskoy i tekstil'noy promyshlennosti // Ekonomika: vchera, segodnya, zavtra. – 2017, № 7. S. 196...204.

Рекомендована кафедрой экономики и управления в строительстве НИМГСУ. Поступила 14.01.19.