Реферат на тему:

**Обеспечение информационной безопасности на промышленном предприятии**

­Выполнил: студент 402 группы

Батунин М. Е.

**Содержание**

|  |  |
| --- | --- |
| 1. Введение |  |
| 1. Понятие информационной безопасности |  |
| 1. Основные угрозы информационной безопасности |  |
| 1. Методы обеспечения информационной безопасности |  |
| 1. Средства обеспечения информационной безопасности |  |
| 1. Автоматизированная система управления технологическим процессом (АСУ ТП) на промышленном предприятии |  |
| 1. Угрозы безопасности промышленных систем |  |
| Уязвимости промышленных АСУ ТП |  |
| 1. Мероприятия по защите промышленных систем |  |
| 1. Заключение |  |
| 1. Источники |  |

**Введение**

Конфиденциальная информация представляет огромный интерес для конкурирующих фирм. Именно она становится причиной посягательств со стороны злоумышленников.

Многие проблемы связаны с недооценкой важности угрозы, в результате чего для предприятия это может обернуться крахом и банкротством. Даже единичный случай халатности рабочего персонала может принести компании многомиллионные убытки и потерю доверия клиентов.

Угрозам подвергаются данные о составе, статусе и деятельности компании. Источниками таких угроз являются её конкуренты, коррупционеры и преступники. Особую ценность для них представляет ознакомление с охраняемой информацией, а также ее модификация в целях причинения финансового ущерба.

К такому исходу может привести утечка информации даже на 20%. Иногда потеря секретов компании может произойти случайно, по неопытности персонала или из-за отсутствия систем защиты.

**Понятие информационной безопасности**

В повседневной жизни часто информационная безопасность (ИБ) понимается лишь как необходимость борьбы с утечкой секретной и распространением ложной и враждебной информации. Однако, это понимание очень узкое. Существует много разных определений информационной безопасности, в которых высвечиваются отдельные её свойства.

В утратившем силу ФЗ «Об информации, информатизации и защите информации» под информационной безопасностью понималось *состояние защищённости информационной среды общества, обеспечивающее её формирование и развитие в интересах граждан, организаций и государства*.

В других источниках приводятся следующие определения:

**Информационная безопасность** – это

1) комплекс организационно-технических мероприятий, обеспечивающих целостность данных и конфиденциальность информации в сочетании с её доступностью для всех авторизованных пользователей;

2) показатель, отражающий статус защищенности информационной системы;

3) состояние защищённости информационной среды;

4) состояние, обеспечивающее защищенность информационных ресурсов и каналов, а также доступа к источникам информации.

В. И. Ярочкин считает, что **информационная безопасность** есть состояние защищённости информационных ресурсов, технологии их формирования и использования, а также прав субъектов информационной деятельности.

Достаточно полное определение дают В. Бетелин и В. Галатенко, которые полагают, что

**Информационная безопасность** –защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам или пользователям информации и поддерживающей инфраструктуры.

ИБ не сводится исключительно к защите информации и компьютерной безопасности. Следует различать информационную безопасность от *защиты информации*.

**Защита информации** – это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.

Иногда под защитой информации понимается создание в ЭВМ и вычислительных системах организованной совокупности средств, методов и мероприятий, предназначенных для предупреждения искажения, уничтожения или несанкционированного использования защищаемой информации.

Меры по обеспечению информационной безопасности должны осуществляться в разных сферах – политике, экономике, обороне, а также на различных уровнях – государственном, региональном, организационном и личностном. Поэтому задачи информационной безопасности на уровне государства отличаются от задач, стоящих перед информационной безопасностью на уровне организации.

**Основные угрозы информационной безопасности**

Под угрозой информационной безопасности понимается случайная или преднамеренная деятельность людей или физическое явление, которые могут привести к нарушению безопасности информации. Далее рассмотрены основные виды и аспекты угроз информационной безопасности.

Все множество потенциальных угроз информационной безопасности по природе их возникновения можно разделить на два класса естественные (объективные) и искусственные (субъективные).

Угрозы безопасности

Естественные

Искусственные

Непреднамеренные

Преднамеренные

*Естественные угрозы* – это угрозы, вызванные воздействиями на автоматизированную систему и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.

*Искусственные угрозы* – это угрозы информационной безопасности, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

1. *Непреднамеренные* (неумышленные, случайные) угрозы, вызванные ошибками в проектировании автоматизированной системы и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.

2. *Преднамеренные* (умышленные) угрозы, связанные с корыстными устремлениями людей (злоумышленников).

Источники угроз по отношению к автоматизированной системе могут быть внешними или внутренними. Внутренние угрозы реализуются компонентами самой информационной системы – аппаратно-программным обеспечением или персоналом.

К основным непреднамеренным искусственным угрозам информационной безопасности относятся действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла:

1. Неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.).

2. Неправомерное отключение оборудования или изменение режимов работы устройств и программ.

3. Неумышленная порча носителей информации.

4. Запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.).

5. Нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях).

6. Заражение компьютера вирусами.

7. Неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной.

8. Разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков).

9. Проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации.

10. Игнорирование организационных ограничений (установленных правил) при работе в системе.

11. Вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.).

12. Некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности.

13. Пересылка данных по ошибочному адресу абонента (устройства).

14. Ввод ошибочных данных.

15. Неумышленное повреждение каналов связи.

К основным преднамеренным искусственным угрозам относятся:

1. Физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.).

2. Отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и др.).

3. Действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.).

4. Внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность).

5. Вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия.

6. Применение подслушивающих устройств, дистанционная фото и видеосъемка и т.п.

7. Перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т.п.).

8. Перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему.

9. Хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПЭВМ).

10. Несанкционированное копирование носителей информации.

11. Хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.).

12. Чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств.

13. Чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме используя недостатки мультизадачных операционных систем и систем программирования.

14. Незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя («маскарад»).

15. Несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.

16. Вскрытие шифров криптозащиты информации.

17. Внедрение аппаратных спец вложений, программных закладок и вирусов, т.е. таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы.

18. Незаконное подключение к линиям связи с целью работы «между строк», с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений.

19. Незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

Чаще всего для достижения поставленной цели злоумышленник использует не один, а некоторую совокупность из перечисленных выше путей.

**Методы обеспечения информационной безопасности**

Основными методами защиты информации являются следующие.

1. **Препятствие** — метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).

2. **Управление доступом** — метод защиты информации регулированием использования всех ресурсов компьютерной информационной системы банковской деятельности (элементов баз данных, программных и технических средств). Управление доступом включает следующие функции защиты:

* идентификацию пользователей, персонала и ресурсов системы
* опознание
* проверку полномочий
* разрешение и создание условий работы в пределах установленного регламента
* регистрацию (протоколирование) обращений к защищаемым ресурсам
* реагирование (сигнализация, отключение, задержка работ, отказ в запросе) на попытки несанкционированных действий с информацией

3. Маскировка — метод защиты информации путем ее криптографического закрытия или её сокрытия, т.е. обеспечения невозможности её найти.

4. Регламентация — метод защиты информации, создающий за счёт организации работ такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

5. Принуждение — такой метод защиты, при котором пользователи и персонал системы вынуждены соблюдать регламенты и правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

6. Побуждение — такой метод защиты, который мотивирует пользователя и персонал системы не разрушать установленные регламенты и порядки за счет соблюдения сложившихся моральных и этических норм (как регламентированных, так и неписаных).

Перечисленные методы обеспечения безопасности реализуются разными средствами, но сущность этих методов остаётся сходной.

**Средства обеспечения информационной безопасности**

Средства обеспечения безопасности – это ресурсы, обеспечивающие безопасность.

К основным средствам защиты, используемым для создания механизма защиты, относятся следующие:

1. *Технические средства* реализуются в виде электрических, электромеханических и электронных устройств. Вся совокупность технических средств делится на аппаратные и физические. Под аппаратными техническими средствами принято понимать устройства, встраиваемые непосредственно в вычислительную технику или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу.

2. *Физические средства* реализуются в виде автономных устройств и систем. Например, замки на дверях, где размещена аппаратура, решетки на окнах, электронно-механическое оборудование охранной сигнализации.

3. *Программные средства* представляют собой программное обеспечение, специально предназначенное для выполнения функций защиты информации.

4. *Организационные средства* защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации вычислительной техники, аппаратуры телекоммуникаций для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы аппаратуры на всех этапах их жизненного.

5. *Морально-этические средства* защиты реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере распространения вычислительной техники и средств связи в обществе. Эти нормы большей частью не являются обязательными как законодательные меры, однако, несоблюдение их ведет обычно к потере авторитета и престижа человека. Наиболее показательным примером таких норм является Кодекс профессионального поведения членов Ассоциаций пользователей ЭВМ США.

6. *Законодательные средства* защиты определяются законодательными актами страны, которыми регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

**Автоматизированная система управления технологическим процессом (АСУ ТП) на промышленном предприятии**

Автоматизированная система управления технологическим процессом (АСУ ТП) – это комплекс программных и технических средств, предназначенный для автоматизации управления технологическим оборудованием на предприятиях.

Под АСУ ТП обычно понимается комплексное решение, обеспечивающее автоматизацию основных технологических операций на производстве в целом или каком-то его участке, выпускающем относительно завершенный продукт. Здесь важно сделать акцент на слове «автоматизированная». Под этим подразумевается, что система управления отнюдь не полностью автономна (самостоятельна), и требуется участие человека (оператора) для реализации определенных задач.

Составными частями АСУТП могут быть отдельные системы автоматического управления (САУ) и автоматизированные устройства, связанные в единый комплекс. Как правило АСУТП имеет единую систему операторского управления технологическим процессом в виде одного или нескольких пультов управления, средства обработки и архивирования информации о ходе процесса, типовые элементы автоматики: датчики, контроллеры, исполнительные устройства. Для информационной связи всех подсистем используются промышленные сети.

Автоматизированные системы управления в настоящее время используются в большинстве отраслей промышленности, в нефте и газодобыче, на электростанциях и железных дорогах, на пивоварнях и лыжных курортах. В мире эксплуатируются миллионы промышленных систем, стоимость которых измеряется тысячами и миллионами долларов США. Степень зависимости критической инфраструктуры государства от таких систем неуклонно возрастает, и вопросы обеспечения их информационной безопасности приобретают первостепенное значение.

В отличие от других видов автоматизированных информационных систем, промышленные системы, особенно те, которые используются для управления критической инфраструктурой, имеют ряд особенностей, обусловленных их особым назначением, условиями эксплуатации, спецификой, обрабатываемой в них информации и требованиями, предъявляемыми к функционированию. Главной же особенностью этих систем является то, что с их помощью в автоматическом, либо полуавтоматическом, режиме в реальном времени осуществляется управление физическими процессами и системами, от которых непосредственным образом зависит наша безопасность и жизнедеятельность: электричество, связь, транспорт, финансы, системы жизнеобеспечения, атомное и химическое производство и т.п.

Обеспечение информационной безопасности промышленных систем требует особого подхода, учитывающего эти особенности. Для того чтобы выработать такой подход, необходимо, прежде всего, оценить серьезность проблемы в целом, затем, опираясь на накопленную статистику инцидентов, подвергнуть тщательному анализу специфические для промышленных систем угрозы и уязвимости и на основании этого анализа определить особые требования к режиму обеспечения информационной безопасности критической инфраструктуры.

**Угрозы безопасности промышленных систем**

Промышленные системы эволюционировали от экзотических программных и аппаратных средств в 70-х до вполне современных систем, в которых используются стандартные IBM-совместимые ПК, операционные системы семейства Microsoft Windows, сетевые протоколы TCP/IP, Web-браузеры, доступ в Интернет. Множество угроз в отношении этих систем значительно расширилось благодаря такой стандартизации, а также благодаря распространенной практике подключения промышленных систем к ЛВС организации и использованию в них технологий беспроводного доступа.

Умышленные угрозы в отношении промышленных систем, в зависимости от того, кто выступает в качестве «*агента угрозы*», можно разделить на следующие основные группы:

* **Вредоносное ПО**. Промышленные системы также, как и любые другие ИТ системы, потенциально подвержены угрозам со стороны компьютерных вирусов, сетевых червей, троянских программ и программ шпионов.
* **Инсайдеры**. Недовольные внутренние пользователи, хорошо знающие систему изнутри, как показывает практика, представляют собой одну из основных угроз. Инсайдер может умышленно повредить оборудование или программное обеспечение. Администраторы и инженеры, обслуживающие систему, могут также неумышленно нанести вред ее функционированию, допустив ошибку в настройках системы или нарушение определенных правил безопасности.
* **Хакеры**. Аутсайдеры могут быть заинтересованы в исследовании возможности получения доступа и контроля над системой, мониторинге трафика и реализации атак на отказ в обслуживании.
* **Террористы**. Это наиболее серьезная угроза, создающая основные различия между системами, относящимися к критической инфраструктуре и обычными ИТ системами. Террористы заинтересованы в том, чтобы вывести систему из строя, нарушить процессы мониторинга и управления, либо получить контроль над системой и нанести как можно больший вред критической инфраструктуре.

К счастью, в критичных отраслях, преимущественно использующих промышленные системы, отсутствуют два основных мотивирующих фактора для киберпреступности. Это экономические стимулы, к которым относятся кредитные карты и электронные счета, лежащие в основе многих компьютерных преступлений, и коммерческие тайны, являющиеся основной целью промышленного шпионажа.

**Уязвимости промышленных АСУ ТП**

На начальном этапе развития в промышленных системах использовалось малоизвестное специализированное оборудование и программное обеспечение, а их сетевое взаимодействие с внешним миром было сильно ограничено. Круг возможных угроз был слишком узок, поэтому внимания вопросам информационной безопасности со стороны разработчиков и владельцев таких систем практически не уделялось. Со временем разработчики переходят на стандартные ИТ платформы, а владельцы промышленных систем, с целью повышения эффективности управления, подключают их к смежным системам. Существующая тенденция к повышению открытости и стандартизации промышленных систем повышает их уязвимость к кибератакам, однако среди экспертов не существует единого мнения относительно того, насколько сложной для аутсайдера задачей является получение доступа к промышленной системе.

В системах критической инфраструктуры существуют те же самые уязвимости, что и в большинстве обычных ИТ систем. Кроме этого, особенности промышленных систем, обуславливают существование в них уникальных уязвимостей, к которым можно отнести:

* **Человеческий фактор**. Эксплуатацией промышленных и корпоративных систем обычно занимаются разные подразделения. Персонал промышленных систем, как правило, достаточно далек от вопросов обеспечения информационной безопасности, в его составе нет соответствующих специалистов, а рекомендации ИТ персонала на него не распространяются. Основной задачей остается решение технологических проблем, возникающих в ходе эксплуатации системы, обеспечение ее надежности и доступности, повышение эффективности и минимизация накладных расходов.
* **Уязвимости операционных систем**. Уязвимости операционных систем в равной степени свойственны и для промышленных и для корпоративных систем, однако установка программных коррекций в промышленных системах на регулярной основе зачастую не выполняется. Главной заботой администратора такой системы является ее бесперебойная работа. Установка предварительно не протестированных программных коррекций может повлечь серьезные неприятности, а на полноценное тестирование обычно нет ни времени, ни средств. На этом сердце администратора и успокаивается.
* **Слабая аутентификация**. Использование общих паролей является обычной практикой для промышленных систем. Благодаря этому у персонала пропадает ощущение подотчетности за свои действия. Системы двухфакторной аутентификации используются довольно редко, а ключевая информация зачастую передается по сети в открытом виде.
* **Удаленный доступ**. Для управления промышленными системами довольно часто используется удаленный доступ по коммутируемым каналам или по VPN каналам через сеть Интернет. Это может привести к серьезным проблемам с безопасностью.
* **Внешние сетевые подключения**. Отсутствие соответствующей нормативной базы и соображения удобства использования порой приводят к тому, что между промышленными и корпоративными системами создаются сетевые подключения. Можно услышать даже рекомендации по поводу использования «комбинированных» сетей, позволяющих упростить администрирование и улучшить безопасность.
* **Средства защиты и мониторинга**. В отличие от корпоративных систем использование IDS, МЭ и антивирусов в промышленных системах не является распространенной практикой, а для анализа журналов аудита безопасности обычно не остается времени.
* **Беспроводные сети**. В промышленных системах часто используются различные виды беспроводной связи, включая протоколы 802.11, как известно, не предоставляющие достаточных возможностей по защите.
* **Удаленные процессоры**. Определенные классы удаленных процессоров, используемых в промышленных системах для контроля технологических процессов, содержат известные уязвимости. Производительность этих процессоров не всегда позволяет реализовать функции безопасности. Кроме того, после установки их стараются не трогать годами, на протяжении которых они остаются уязвимыми.
* **Программное обеспечение**. Программное обеспечение промышленных систем обычно не содержит достаточного количества функций безопасности. Кроме того, оно не лишено архитектурных слабостей.
* **Раскрытие информации**. Не редко владельцы промышленных систем сознательно публикуют информацию об их архитектуре. Консультанты и разработчики частенько делятся опытом и раскрывают информацию о бывших клиентах.
* **Физическая безопасность**. Удаленные процессоры и оборудование промышленных систем могут находиться за пределами контролируемой зоны. В таких условиях, они не могут физически контролироваться персоналом, и единственным механизмом физической защиты становится использование железных замков и дверей, а такие меры уж точно не являются серьезным препятствием для террористов.

Мы видим, что существует значительное количество уязвимостей, являющихся специфичными для промышленных систем. Эти уязвимости обуславливают особые требования по безопасности и особые режимы эксплуатации таких систем.

**Мероприятия по защите промышленных систем**

Формирование взглядов и приоритетов в области обеспечения информационной безопасности промышленных систем критической инфраструктуры хорошо прослеживается на примере США – страны, в наибольшей степени подверженной угрозам кибертерроризма. В 1997 году на свет появился отчет Президентской комиссии по защите критической инфраструктуры, который послужил точкой отсчета для начала широкомасштабных действий, предпринимаемых правительством США с целью повышения защищенности физической, сетевой и информационной инфраструктуры государства. В 1998 году Указ Президента США №63 (PDD63) определил понятие критической инфраструктуры как «физические и информационные системы, необходимые для обеспечения минимально допустимого уровня функционирования экономики и правительства». К критической инфраструктуре были отнесены: телекоммуникации, энергетика, банковская и финансовая система, транспорт, водные системы и аварийные службы. PDD63 также определил основные элементы государственной стратегии в области защиты критической инфраструктуры, к числу которых относятся:

* Важность сотрудничества между общественным и частным сектором
* Головные федеральные агентства для каждого сектора критической инфраструктуры
* Координационные группы для координации усилий федеральных агентств и промышленных групп
* Система оповещения и обмена информацией в рамках Национального центра защиты инфраструктуры (NIPC)
* Системы обмена информацией для каждого сектора промышленности, известные как Центры сбора и анализа информации (ISAC)
* Требование создания «Плана обеспечения безопасности национальной инфраструктуры», устанавливающего контрольные точки для анализа уязвимостей и подготовки планов их ликвидации в каждом секторе промышленности.

В 2001 году после известных событий 11 сентября был выпущен «Акт о защите критической инфраструктуры», а в 2002 году «Акт о безопасности Отечества», в соответствии с которым в США был образован Департамент национальной безопасности (DHS) и учреждена должность Директора по анализу информации и защите инфраструктуры. В 2003 году Президентом США была утверждена «Национальная стратегия обеспечения безопасности киберпространстра». Этот объемный документ адресован широкой американской общественности и направлен на расширение взаимодействия и консолидацию усилий различных слоев общества, государственных, общественных и частных организаций в деле противодействия кибертерроризму. Основная часть Стратегии расставляет приоритеты по созданию системы ответных мер, программы противодействия угрозам и уязвимостям, программы обучения и повышения осведомленности, национальной и международной кооперации. Повышение защищенности промышленных систем было объявлено национальным приоритетом.

С этого времени в мероприятиях по обеспечению безопасности промышленных систем задействованы разработчики и владельцы этих систем, консультанты и научно-исследовательские организации, независимые ассоциации и государственные учреждения. Для отработки технических решений по защите промышленных систем были созданы тестовые лаборатории (например, National SCADA Test Bed). В результате было выпущено и продолжается разработка значительного количества стандартов и руководств по различным аспектам обеспечения безопасности промышленных систем.

Компанией Digital Bond Inc. был разработан «Профиль защиты центра управления для промышленных систем управления», в котором формализуется перечень из 22 видов угроз в отношении центра управления промышленных систем, на основании данного перечня формулируются 28 задач защиты, исходя из которых определяется 55 компонентов функциональных требований безопасности и 17 компонентов требований к гарантированности оценки в соответствии с Общими Критериями (4). Этой компанией был также разработан набор сигнатур сетевых атак для протоколов Modbus TCP и DNP3, используемых в промышленных системах. Эти сигнатуры изначально были разработаны для системы Snort в рамках исследовательского проекта, финансируемого Департаментом Национальной Безопасности США. Поддержка сигнатур была добавлена в соответствующие продукты Symantec и ISS, являющихся лидерами в этом сегменте рынка информационной безопасности. Компания Cisco модифицировала эти сигнатуры для работы на своей платформе (они были включены в S198 Signature Update для Cisco IDS версии 4.1 и IPS версии 5.0). Продолжается исследовательская работа по созданию механизмов защиты и для других распространенных сетевых протоколов, используемых в промышленных системах.

В ходе планирования и реализации организационно-технических мер по защите промышленных систем необходимо, прежде всего, опираться на международные стандарты ИБ, наиболее востребованным из которых в настоящее время является ISO/IEC 17799:2005. Учитывая повышенные требования по защите критической инфраструктуры, в дополнение к существующим международным стандартам, определяющим только базовые механизмы безопасности, необходимо применять также специализированные стандарты и руководства, появившиеся на свет благодаря широкомасштабным мероприятиям по защите критической инфраструктуры, проводимым в США, такие как “Urgent Action Standard 1200 – Cyber Security”, Cryptographic Protection of SCADA Communications, Part 1: Background, Policies, and Test Plan” и многие др.

**Заключение**

Защита промышленных систем критической инфраструктуры от кибератак постепенно становится одним из высших приоритетов в обеспечении государственной безопасности. Когда повышенный уровень террористической угрозы сочетается со стремительно возрастающим уровнем зависимости общества от промышленных систем, этот вопрос стоит особенно остро и требует от правительства принятия скоординированных всеобъемлющих мер. И хотя кибертеррористических актов на сегодня фактически зафиксировано не было, угроза представляется вполне реальной.

Для большинства промышленных систем присущи уязвимости, характерные и для других ИТ систем, а также уязвимости, являющиеся для них специфическими. Для обеспечения адекватной защиты таких систем их разработчики должны будут предпринять значительные усилия по повышению уровня защищенности своих продуктов, встраиванию в них функций безопасности в соответствии с требованиями специализированных профилей защиты с последующей их сертификацией. Владельцы и организации, эксплуатирующие промышленные системы, должны будут изменить свое отношение к вопросам информационной безопасности и существующую систему приоритетов в этой области.

Важнейшая роль в решении вопросов безопасности промышленных систем критической инфраструктуры будет принадлежать правительству, органам государственной безопасности и антитеррористическим структурам. Для проведения соответствующих научно-исследовательских работ, разработки стандартов, методологий и средств защиты промышленных систем потребуются значительные объемы государственного финансирования, масштабные государственные программы и правовое регулирование.

**Источники**

1. Гафнер В.В. Информационная безопасность: учеб. пособие / В.В. Гафнер. – Ростов на Дону: Феникс, 2010. - 324 с.
2. Александр Астахов, Реалии и мифы кибертерроризма, Открытые системы № 5, 2003
3. Интернет источник. Ссылка: https://otherreferats.allbest.ru/physics/00228787\_0
4. Интернет источник. Ссылка: <https://studfiles.net/preview/5785046/>
5. Интернет источник. Ссылка: <https://studfiles.net/preview/5247352/>