www.volsu.ru

# ИННОВАЦИИ В ИНФОРМАТИКЕ, ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКЕ И УПРАВЛЕНИИ

DOI: https://doi.org/10.15688/NBIT.jvolsu.2020.2.1

УДК 681.518:004.491
ББК 32.966

## АНАЛИЗ ИНФОРМАЦИОННЫХ УГРОЗ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ

**Григорий Владимирович Жарков**

Студент, кафедра информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

**Вадим Юрьевич Шевцов**

Ассистент, кафедра информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

**Аннотация.** Определена актуальность информационной безопасности промышленных предприятий. Рассматриваемые угрозы информационной безопасности автоматизированных систем управления технологическими процессами сгруппированы по их источникам, а также по признаку преднамеренности их возникновения. Приведены некоторые примечательные инциденты безопасности. Сделан вывод о необходимости повышения защищенности информационных систем промышленных предприятий.

**Ключевые слова:** информационная безопасность предприятия, промышленная безопасность, угрозы, риск, вредоносный USB-носитель.



Информационная безопасность предприятия (ИБ предприятия) – это состояние защищенности данных, объектов информатизации предприятия и его интересов. ИБ предприятия будет достигнуто только при выполнении таких свойств основных свойств ИБ, как конфиденциальность, целостность, доступность информации и технической составляющей

предприятия, задействованных в технологических процессах [1].

ИБ предприятия осуществляется с применением как организационных, так и технических мер, нацеленных на обеспечение защиты информационных ресурсов. Организационные меры содержат политики ИБ для работы с различными категориями и видами информации, ИТ-сервисами, средствами защиты и т. д. Технические меры для защиты информации включают в себя как программные, так и программно-аппаратные средства для осуществления следующих функций: контроль доступа, мониторинг системы от утечек информации, обнаружения вторжений на территорию предприятия, системы видеонаблюдения, антивирусная защита, межсетевое экранирование, защита от электромагнитных излучений и прочее.

Задачи систем информационной безопасности предприятия многообразны. Вот лишь некоторые из них:

1) обеспечение защищенного хранения информации;

2) защита передачи информации по компьютерным сетям;

3) разграничение доступа к различным информационным ресурсам;

4) резервное копирование и восстановление информационных систем.

Обеспечение ИБ предприятия будет эффективным только при системном и комплексном подходе к защите. В системе ИБ должны учитываться все актуальные информационные угрозы и уязвимости.

Полноценная информационная безопасность предприятий и организаций подразумевает постоянный контроль важных событий и состояний, оказывающих влияние на информацию предприятия. Защита должна осуществляться непрерывно и полностью включать жизненный цикл информации – от ее возникновения до уничтожения или потери актуальности.

ИБ осуществляется соответствующей службой предприятия в кооперации с отделом информационных технологий, экономической безопасности, кадров и другими службами.

Угрозы информационной безопасности анализируются для определения полного набора требований к разрабатываемой системе защиты. Обычно под угрозой понимают потенциально возможное действие, результат которого может нанести ущерб объектам защиты. В ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» приведено следующее определение угрозы информационной безопасности: «Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации» [2]. Угроза считается актуальной, если она может быть реализована в информационной системе предприятия и представляет опасность для информации ограниченного доступа. Угрозы информационной безопасности определяются по результатам анализа, включающего:

• оценку возможностей внешних и внутренних нарушителей;

• перечень возможных уязвимостей ИС;

• перечень способов реализации угроз;

• расчет теоретически возможного ущерба от нарушения конфиденциальности, целостности, доступности информации предприятия.

Далее приводятся актуальные угрозы ИБ промышленных предприятий.

1) *Непреднамеренные действия сотрудников.* Угрозу ИБ предприятия могут представлять даже лояльные и ответственные сотрудники. Непредумышленный вред конфиденциальной информации возможен по безбрежности или неосведомленности персонала. Существует потенциальная возможность открытия фишингового письма, которое внедрит вирус с личного ноутбука на сервер компании. Также возможна утечка конфиденциальной информации в целях злоумышленников. Нет предприятий, абсолютно защищенных от передачи невнимательным сотрудником важных файлов не тому адресату. В такой ситуации информация оказывается весьма легкой добычей.

Так, киберпреступники, используя зловред (программу-вымогатель), произвели взлом сети (обслуживаемой компанией Ameren) компании поставщика оборудования для энергетики LTI Power Systems, зарегистрированной в штате Огайо, и получили доступ к конфиденциальным сведениям.

Злоумышленники смогли выкрасть технические характеристики систем бесперебойного питания, которые необходимы во время

прекращения подачи регулярной энергии. Украденные документы датировались периодом с 1996 по 2017 год.

Обеспечение безопасности сторонних поставщиков является серьезной проблемой, в связи с тем, что атаки становятся все более изощренными [5].

2) *Использование уязвимого ПО и оборудования.* Иногда руководители предприятий пытаются сэкономить на покупке качественного ПО и оборудования или замене устаревшего. Но необходимо учитывать, что устаревшее и не прошедшее аудит ПО не дает защиты от мошенников, заинтересованных в краже информации с помощью вирусов. Обладатель такого ПО часто не получает технической поддержки, своевременных обновлений, предоставляемых компаниями-разработчиками. Но даже надежное проприетарное ПО может оказаться «троянским конем», что необходимо учитывать при его использовании.

11 февраля 2020 года был выявлен факт, что Центральное разведывательное управление США (ЦРУ) и Федеральная разведывательная служба Германии (BND) более полу века имели доступ к защищенным перепискам по всему миру. Для этого они использовали оборудование швейцарской компании Crypto AG.

О факте несанкционированного доступа к таким каналам сообщило издание Washington Post (WP) после изучения отчета центра ЦРУ по разведке за 2004 год, а также благодаря интервью бывших разведчиков из BND.

Crypto AG выпускало продукцию двух видов – защищенное и уязвимое. Безопасная версия продуктов распространялась в Швейцарии и некоторых других странах. Остальные государства получали оборудование с недекларированными возможностями для тайного съема информации [6].

3) *Недобросовестные сотрудники.* Именно легальные пользователи – одна из основных причин утечек информации в компаниях. Такие утечки специалисты называют инсайдерскими, а всех инсайдеров условно делят на несколько групп: нарушители, злоумышленники, кроты, обиженные сотрудники.

Федеральный суд США приговорил Кристофера Айвса, бывшего сотрудника компании Gearbox Studios, к одному году тюрьмы. Чтобы отомстить за увольнение Айвс устроил кибератаку, в ходе которой безвозвратно уничтожил и исказил множество файлов, а также украл информацию о клиентах.

Вскоре после своего увольнения, Айвс решил насолить бывшему работодателю и в период с февраля по май 2015 г. совершил серию умышленных действий в отношении информационных активов Gearbox. В частности, он удалил данные 177 из 200 клиентских сайтов – всего порядка 20 тыс. записей о продуктах. После его вмешательства стоимость отдельных продуктов для клиентов «упала» до $1–2 [4].

4) *Угроза атак злоумышленников*. Самый серьезный источник угрозы для любого предприятия. Существуют как самостоятельные, так и специальные группы взломщиков. Цели данных групп различны: от обычного шантажа до промышленно саботажа и кражи секретной информации. Самостоятельные группировки чаще всего занимаются раскрытием секретной информации для общественности или взломом лицензированного ПО и предоставлением свободного доступа к нему.

FIN7 – группировка хакеров, которая атакует организации, через почту США вредоносные USB-накопители. Эти устройства при подключении к компьютеру ведут себя как клавиатура, что позволяет злоумышленникам выполнять команды и устанавливать JavaScript-бэкдор.

Этот формат проникновения на устройства напоминает так называемый «lost USB», используемый пентестерами в своих целях (см. рисунок).

Один из клиентов Trustwave получил посылку якобы от сети магазинов Best Buy, которая предлагала подарочный сертификат на $50 по программе лояльности. В конверте также находилось USB-устройство, на котором должен быть размещен список продуктов, доступных для оплаты вышеупомянутым сертификатом.

Самая главная составляющая атак – USB-накопитель, позволяющий выполнять заранее заданные действия при помощи эмуляции работы клавиатуры. Таким образом, устройство может запускать команды PowerShell, помогающие загрузить вредоносную программу с командного сервера, которым управляют операторы FIN7 [3].

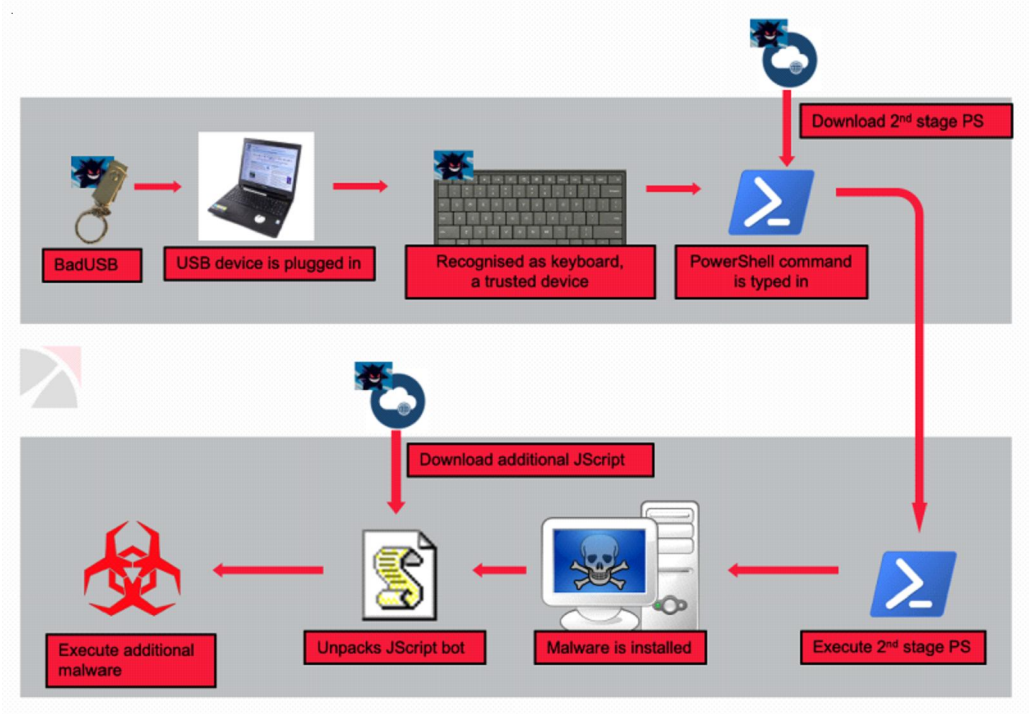


Рисунок. Схема работы вредоносного USB-накопителя

5) *Утечка информации через технические каналы*. Утечка информации – это неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации. Источником угрозы утечки информации по техническим каналам могут быть как разнообразные технические средства, так и посторонние лица – нарушители безопасности информации. В соответствии с базовой моделью угроз безопасности информации к техническим каналам утечки информации обычно относятся:

- каналы утечки речевой информации;
- каналы утечки визуальной информации.

6) *Угроза типа отказ в обслуживании*. Суть угрозы в том, что для обработки каждого сетевого запроса системой потребляется часть ее ресурсов, что, в свою очередь, означает возможность отказа дискредитированной системой в доступе легальным пользователям при лавинообразном увеличении числа сетевых соединений с данной системой и при использовании недостатков реализации сетевых протоколов.

Круг угроз ИБ промышленного предприятия очень широк и ограничивается не только рассмотренными в данной статье. Очень важно соблюдать высокий уровень ИБ предприятия особенно на объектах критической информационной инфраструктуры (КИИ).

## *СПИСОК ЛИТЕРАТУРЫ*

1. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – М. : Стандартинформ, 2009. – 20 с.

2. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Электрон. дан. – Режим доступа: http://docs.cntd.ru/document/1200058320. – Загл. с экрана.

3. Группировка FIN7 рассылает компаниям вредоносные USB-устройства. – Электрон. дан. – Режим доступа: https://www.anti-malware.ru/news/2020-03-30-1447/32332. – Загл. с экрана.

4. Программист сядет в тюрьму за атаку на бывшего работодателя. – Электрон. дан. – Режим доступа: https://www.infowatch.ru/analytics/data-loss-cases/21090. – Загл. с экрана.

5. Хакеры завладели данными о двух электростанциях. – Электрон. дан. – 25.03.2020. – Режим доступа: https://www.infowatch.ru/analytics/data-loss-cases/22834. – Загл. с экрана.

6. 2020: Спецслужбы США и Германии 50 лет следили за перепиской 120 стран, контролируя Crypto AG. – Электрон. дан. – Режим доступа: http://www.tadviser.ru/index.php/Компания:Crypto_AG аналитическое агенство TAdviser. – Загл. с экрана.

***REFERENCES***

1. *GOST R 53114-2008 Information security. Ensuring information security in the organization. Basic terms and definitions*. Moscow, Standartinform Publ., 2009. 20 p.

2. *GOST R 50922-2006*. URL: http://docs.cntd.ru/document/1200058320.

3. *The FIN7 group is sending malicious USB devices to companies*. URL: https://www.anti-malware.ru/news/2020-03-30-1447/32332.

4. *The programmer goes to jail for attacking a former employer*. URL: https://www.infowatch.ru/analytics/data-loss-cases/21090.

5. *Hackers got hold of data on two power plants.* URL: https://www.infowatch.ru/analytics/data-loss-cases/22834 InfoWatch analytical resource 03/25/2020.

6. *2020: The special services of the USA and Germany have been following the correspondence of 120 countries for 50 years, controlling Crypto AG*. URL: http://www.tadviser.ru/index.php. Company: Crypto_AG analytical agency TAdviser.

# ANALYSIS OF INFORMATION THREATS TO INDUSTRIAL SECURITY

**Grigory V. Zharkov**

Student, Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

**Vadim Yu. Shevtsov**

Assistant Lecturer, Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

**Abstract.** Information security of an enterprise (IS of an enterprise) is the state of security of data, objects of informatization of an enterprise and its interests. IS of an enterprise is achieved only when such properties of the basic properties of IS as confidentiality, integrity, availability of information and the technical component of an enterprise involved in technological processes are met. Ensuring IS of an enterprise is effective only with a systematic and comprehensive approach to protection. The information security system should take into account all current information threats and vulnerabilities. Information security threats are analyzed to determine the full set of requirements for the developed security system. A threat is considered relevant if it can be implemented in the information system of the enterprise and poses a threat to information with limited access. It is shown that the list of threats to information security of an industrial enterprise is very wide and is limited not only to those considered in this article. It is very important to maintain a high level of enterprise information security, especially at critical information infrastructure facilities.

**Key words:** company information security, industrial security, threats, risk, badUSB.