УДК 004.56:388.45.01

МЕТОДЫ ОЦЕНКИ ИССЛЕДОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КОМПЬЮТЕРНЫХ УГРОЗ

***Санжаров Айдар Санжарович**, магистр ИТССм-1-16, Институт Электроники и Телекоммуникация при КГТУ имени И.Раззакова, Кыргызская Республика 720044, Бишкек, Проспект Ч.Айтматова 66, e-mail: aidar_san@mail.ru*
***Баракова Жанна Токтобековна**, к.т.н.,доцент, Институт Электроники и Телекоммуникация при КГТУ имени И.Раззакова, Кыргызская Республика 720044, Бишкек, Проспект Ч.Айтматова 66, e-mail: janna05_05@mail.ru*

Аннотация.В статье рассмотрена разработка методов исследования, для решения компьютерных угроз и атак информационной безопасности, является одной из важнейших тем на сегодняшний день. Так как информационные технологии встречаются во всех отраслях промышленности, с которыми мы встречаемся. Соответственно данные которые мы храним должна быть готова к различным угрозам и атакам. Уделено особенное внимание на информационной безопасности в медицинской отрасли. Описано как исследовательские центры отслеживают группы злоумышленников, к каким методам злоумышленники выходят, если предпринятые меры им не помогают. Автором проведен анализ информационной безопасности и возможные атаки на промышленные отрасли.

Ключевые слова: автоматизированные системы, информационная безопасность, Advanced Persistent Threat (сложная постоянная угроза или целевая кибератака), программное обеспечение, средство массовой информации, Information Technology.

METHODS OF ESTIMATION OF RESEARCHES OF INFORMATION SECURITY AND COMPUTER THREATS

Sanzharov Aidar Sanzharovich, *Master Student of ITSSm-1-16, Electronics and Telecommunication Institute under the KSTU named after I.Razzakov; 66, Ch.Aitmatov Prospect, Bishkek, Kyrgyz Republic 720044; e-mail: aidar_san@mail.ru*
Barakova Zhanna Toktobekovna*, Ph.D., Associate Professor, Electronics and Telecommunication Institute under the KSTU named after I.Razzakov; 66, Ch.Aitmatov Prospect, Bishkek, Kyrgyz Republic 720044; e-mail: janna05_05@mail.ru*

Abstract The article considers the development of research methods, for solving computer threats and information security attacks, is one of the most important topics for today. Since information technology is found in all industries with which we meet. Accordingly, the data we store must be ready for various threats and attacks. Particular attention is paid to information security in the medical industry. It describes how research centers track groups of intruders, to which methods attackers leave, if the measures taken do not help them. The author conducted an analysis of information security and possible attacks on industrial sectors.

Key words: automated systems, information security, Advanced Persistent Threat, software, media, Information Technology.

Введение

Современным этапом развития защиты информации характеризуется переходом от традиционного представления к более широкому пониманию информационной безопасности. Новое представление заключается в реализации комплексного подхода основному направлению: защиты информации. В свою очередь, защита информации приобретает международный масштаб и стратегический характер, она становится одной из ключевых современных проблем. При этом выделяют три основных направления защиты информационных воздействий: на информационные системы и средства, общество и психику человека. Однако, в обеспечении ИБ этот вид угроз сегодня не достаточно учитывается. В соответствии с этим обеспечение информационной безопасности автоматизированных систем (АС) является важным и определяет необходимость разработки правильных методов и моделей обеспечения ИБ автоматизированных систем в профессиональной деятельности [1].

Вместе с тем АС, специфики своей профессиональной деятельности, подвержены внешним информационным воздействиям, последствия которых могут носить тяжелый характер. Поэтому своевременное обнаружение потенциальных информационных угроз для АС различного уровня может быть определено своевременными действиями по выявлению и пресечению специальных информационных воздействий. Выявление индивидуальных реакций АС возможно только при внедрении динамических методов анализа физиологического и функционального состояния непосредственно в условиях профессиональной деятельности [1].

Информационная безопасность

Информационная безопасность – это средства защиты информации от случайного или преднамеренного воздействия. Независимо от того, что лежит в основе воздействия: естественные факторы или причины искусственного характера – владелец информации несет убытки [2].

Целостность - информационных данных означает способность информации сохранять изначальный вид и структуру как в процессе хранения, как и после неоднократной передачи. Вносить изменения, удалять или дополнять информацию вправе только владелец или пользователь с правом доступа к данным.

Конфиденциальность – характеристика, которая указывает на необходимость ограничить доступа к информационным ресурсам для определенного круга лиц. В процессе действий и операций информация становится доступной только пользователям, который включены в информационные системы и успешно прошли идентификацию.

Доступность - информационных ресурсов означает, что информация, которая находится в свободном доступе, должна предоставляться полноправным пользователям ресурсов своевременно и беспрепятственно.

Достоверность - указывает на принадлежность информации доверенному лицу или владельцу, который одновременно выступает в роли источника информации [2].

Больше атак

Глобальные центры исследования и анализа угроз всех компаний отслеживает более 100 APT-групп. Некоторые группировки обладают богатыми возможностями и широчайшим арсеналом средств атаки. Иногда они используют традиционные методы взлома, а потом передают работу более опытным командам хакеров. Нередко мы наблюдали ситуации, когда опытные хакеры долго пытались взломать определенную цель и каждый раз уходили ни с чем. Такую стойкость потенциальной жертвы можно объяснить либо наличием мощного защитного решения и обученных сотрудников, не поддающихся на методы социальной инженерии, либо тщательной проработкой продуманной стратегией по противодействию APT-атакам, подготовленных для защиты. Как правило, опытные и настойчивые злоумышленники, специализирующиеся на APT-атаках, просто так не сдаются — они продолжают искать бреши в защите, пока не найдут [3].

Если все предпринятые меры не приносят плодов, злоумышленники временно отступают, чтобы повторно оценить свою цель. В итоге киберпреступники могут прийти к выводу, что атака на цепочку поставок может оказаться эффективнее прямого наступления. Даже если сеть организации со всех сторон прикрыта наилучшими в мире средствами защиты, ее сотрудникам все равно приходится работать со сторонним ПО. Взломав более простое и уязвимое стороннее решение, можно проскользнуть за надежные рубежи защиты исходной цели [3].

Угрозы в автомобильной отрасли.

Современные автомобили — это уже не просто электромеханический транспорт. С каждым последующим поколением происходит интеграция интеллектуальных и коммуникационных технологий в автомобили, что, в свою очередь, делает их умнее, эффективнее, комфортнее и безопаснее. Рынок «подключенных» автомобилей увеличивается, демонстрируя годовой темп роста в 10 раз быстрее общего рынка автомобилей [4].

Удаленная диагностика неисправностей, информационно-развлекательные системы с выходом в Интернет значительно повышают комфорт и безопасность водителя, но вместе с тем представляют новый вызов для всей автомобильной отрасли, так как превращают автомобиль в очередную цель для кибератак. С учетом растущего риска взлома автомобиля, ставящего под удар приватность водителя, его безопасность и сохранность вложений, производителям важно понять уровень угрозы и заняться IT-безопасностью [4].

Автомобильная отрасль может столкнутся со следующими угрозами:

- Уязвимости, возникающие по невнимательности или некомпетентности производителя, усугубляемые конкурентным давлением.
- Уязвимости, возникающие по причине повышенной сложности продукта и сервисов.
- Ни один программный код нельзя на 100% защитить от системных ошибок.
- ПО будут создавать разные разработчики, устанавливать разные поставщики, и оно будет опираться на различные платформы управления. В итоге ни у кого из участников не будет полной картины исходного кода автомобиля.
- Приложения работают на киберпреступников.

- «Подключенные» компоненты все чаще разрабатываются и внедряются компаниями, более знакомыми с аппаратным, чем с программным обеспечением. Как правило, такие компании недооценивают важность постоянных обновлений.
- «Подключенные» автомобили будут создавать и обрабатывать еще больше информации как о самом автомобиле, так и о водителе. Злоумышленники будут продавать эти данные на черном рынке или использовать их для шантажа и вымогательства [4].

Угрозы в отрасли медицины.

Количество угроз в отрасли здравоохранения будет возрастать одновременно с количеством «подключенных» устройств и уязвимых веб-приложений. Развитие отрасли «подключенной» медицины обусловлено рядом факторов. Это потребность в ресурсах и их эффективном использовании; острая необходимость в удаленном, домашнем уходе при хронических заболеваниях, таких как диабет, или заботе о пожилых людях; желание людей вести здоровый образ жизни; польза совместного доступа разных учреждений к данным и отслеживаемым показателям пациента, что значительно улучшает качество и эффективность медицинского ухода [5].

Медицинская отрасль может столкнутся со следующими угрозами:

- Увеличение количества атак на медицинское оборудование для организации вредоносных сбоев, вымогательства или других преступных действий.
- Вырастет количество целевых атак с целью кражи данных.
- Возникнет еще больше инцидентов, связанных с атаками программ-вымогателей на учреждения здравоохранения.
- В медицинских учреждениях станет еще сложнее соблюдать четко заданный корпоративный периметр, так как все больше рабочих станций, серверов, мобильных устройств и оборудования будут подключены к Интернету.
- Целью преступников станет перехват личных и конфиденциальных данных между «умными» носимыми устройствами, например, имплантами, и медработниками**.**
- Общегосударственные и региональные системы здравоохранения, передающие в незашифрованном или незащищенном виде данные между частными специалистами, больницами, клиниками и другими учреждениями, — легкая мишень для злоумышленников, которые перехватывают данные в обход корпоративных сетевых экранов**.**
- Широкая распространенность фитнес-гаджетов и других «подключенных» устройств для здорового образа жизни позволяет киберпреступникам похищать персональные данные, преодолев минимальную защиту.
- Деструктивные атаки, будь то DoS-атаки или уничтожение данных через программы-вайперы (такие как WannaCry), станут серьезной угрозой цифровым системам медицинских учреждений.
- Развивающиеся технологии, такие как интеллектуальные искусственные конечности и импланты для физиологических улучшений или встроенной дополненной реальности [5].

Угрозы в финансовой отрасли.

С помощью вредоносных программ злоумышленники получили возможность манипулировать приложениями, отвечающими за трансграничные транзакции и по сути открыли возможность выводить деньги из любой финансовой организации мира, ведь это ПО унифицировано и им пользуются практически все крупные игроки финансового рынка. Жертвами подобных атак стал ряд банков из более чем 10 стран мира [6].

Спектр связанных с финансами организаций, в которые старались проникнуть киберпреступники, значительно расширился. Различные группировки проникали в

инфраструктуру банков, систем электронных денег, бирж крипто валют, фондов управления капиталом и даже казино с целью вывода очень крупных сумм денег.

Последние несколько лет количество и качество атак, нацеленных на организации финансового сектора, растет непрерывно. Речь идет об атаках именно на инфраструктуру и сотрудников самой организации, а не её клиентов. Мы пришли к ситуации, когда те финансовые учреждения, которые не подумали о защите от хакерских атак, уже в ближайшем времени столкнутся с последствиями вторжения киберзлоумышленников. Результатом станет полная остановка, а затем и потеря бизнеса [6].

Для предотвращения подобной ситуации необходимо постоянно адаптировать свои системы безопасности к новым возникающим угрозам, что невозможно без анализа данных о наиболее важных и релевантных кибератаках, нацеленных на финансовые организации.

Финансовая отрасль может столкнутся со следующими угрозами:

- Появление атак на банковские системы, построенные на блокчейне, через уязвимости и ошибки в этой технологии
- Новые инциденты, связанные с проникновением в сеть финансовой организации через взлом поставщиков ПО
- Манипулирование и взломы СМИ и социальных медиа (Twitter, Facebook, каналы Telegram) ради извлечения прибыли из спровоцированных информационными фальшивками рыночных колебаний
- Автоматизация вредоносного ПО для банкоматов
- Новые атаки на крипто валютные биржи
- Резкий рост «традиционного» мошенничества с платёжной информацией, спровоцированный массовыми утечками данных в 2017
- Увеличение количества атак на финансовые организации со стороны спонсируемых государствами группировок хакеров [6].

Угрозы в сфере промышленной безопасности.

2017 год был одним из самых насыщенных в плане инцидентов, связанных с информационной безопасностью промышленных систем. Эксперты по безопасности обнаружили сотни новых уязвимостей, исследовали новые атаки на технологические процессы, собрали и проанализировали статистику случайных заражений промышленных систем и обнаружили целевые атаки на промышленные предприятия [7].

Однако наиболее значительной угрозой для промышленных систем в 2017 году стали атаки шифровальщиков-вымогателей. Первой половине года промышленные информационные системы в 63-х странах мира подверглись множественным атакам с использованием программ-шифровальщиков. Судя по всему, разрушительные атаки программ-вымогателей WannaCry и ExPetr навсегда изменили отношение промышленных предприятий к проблеме защиты ключевых производственных систем [7].

Отрасль в сфере промышленности может столкнутся со следующими угрозами:

- Рост числа случайных заражений вредоносным ПО.
- Увеличение риска целевых атак с применением программ-вымогателей.
- Увеличение числа инцидентов, связанных с промышленным кибершпионажем.
- Новые сегменты подпольного рынка, обслуживающие атаки на промышленные системы.
- Появление новых видов вредоносного ПО и вредоносных инструментов.
- Использование преступниками результатов анализа угроз, обнародованных исследователями безопасности.
- Изменения в нормативной базе.
- Формирование рынка страхования промышленных предприятий от кибер-рисков и рост инвестиций в этот вид страхования [7].

Заключение

Для достижения цели информационной защищенности, необходимо учесть следующие задачи:

- анализ современного состояния зарубежных и отечественных средств защиты информации;
- исследование возможных угроз информации;
- разработка модели и алгоритмов оценки текущей информационной безопасности;
- экспериментальная проверка предложенных моделей и методов оценки информационной защищенности.

Опытные киберпреступники будут проводить оригинальные и необычные атаки и осваивая новый. Ежегодные темы и тренды не стоит рассматривать отдельно друг от друга – они тесно взаимодействуют, образуя ландшафт угрозы безопасности, актуальный для всех, от пользователей до бизнеса и правительств. Мы не знаем, когда это закончится, но знания об угрозах и их понимание будут мощными инструментами в ваших руках.

Список литературы

1. Модель и методы оценки информационной защищенности оператора автоматизированных систем: http://tekhnosfera.com/model-i-metody-otsenki-informatsionnoy-zaschischennosti-operatora-avtomatizirovannyh-sistem (дата обращения 30.03.2018).

2. Информационная безопасность https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti/

3. Лаборатория Касперского https://securelist.ru/ksb-threat-predictions-for-2018/88032/ (дата обращения 30.03.2018).

4. Прогнозы по развитию компьютерных угроз в автомобильной отрасли https://securelist.ru/ksb-threat-predictions-for-automotive-in-2018/88036/ (дата обращения 20.04.2018).

5. Прогнозы атак в отрасли медицины https://securelist.ru/ksb-threat-predictions-for-connected-health-in-2018/88038/ (дата обращения 25.04.2018).

6. Киберпреступники против финансовой организации https://securelist.ru/ksb-threat-predictions-for-financial-services-and-fraud-in-2018/88040/ (дата обращения 30.04.2018).

7. Прогнозы по развитию угроз в сфере промышленной безопасности https://securelist.ru/ksb-threat-predictions-for-industrial-security-in-2018/88042/ (дата обращения 1.05.2018).

References

1. Model and methods for assessing the information security of the operator of automated systems: http://tekhnosfera.com/model-i-metody-otsenki-informatsionnoy-zaschischennosti-operatora-avtomatizirovannyh-sistem (accessed 30 March 2018).

2. Information security https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti/

3. Kaspersky Lab https://securelist.ru/ksb-threat-predictions-for-2018/88032/ (accessed 30 March 2018).

4. Forecasts for the development of computer threats in the automotive industry https://securelist.ru/ksb-threat-predictions-for-automotive-in-2018/88036/ (accessed April 2018).

5. Forecasts of attacks in the medical industry https://securelist.ru/ksb-threat-predictions-for-connected-health-in-2018/88038/ (accessed 25 April 2018).

6. Cybercriminals against a financial institution https://securelist.ru/ksb-threat-predictions-for-financial-services-and-fraud-in-2018/88040/ (accessed 30 April 2018).

7. Forecasts on development of threats in the sphere of industrial safety https://securelist.ru/ksb-threat-predictions-for-industrial-security-in-2018/88042/ (accessed 1 May 2018).