РАЗРАБОТКА ЗАЩИТЫ КОМПЬЮТЕРНОЙ СЕТИ ОТ УГРОЗ ИЗ ВНЕШНЕЙ СРЕДЫ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Сорокин С.А., Гурин И.А.

Вишняков В.А – д.т.н., профессор

Согласно отчету лаборатории Касперского III квартал 2015 года характеризовался значительно возросшим количеством атак хакеров, направленных на отказ работы информационных систем. Причём география подобных сетевых угроз достаточно широка – DDoS-атакам подвергались цели в 79 странах мира. При этом 91 % атакованных ресурсов приходится на 10 стран мира. Лидерами по количеству DDoS-атак являются США, Китай и Республика Корея. Кроме широкого географического распространения, следует отметить огромное количество аппаратных и финансовых ресурсов, потраченных на некоторые сетевые атаки. В 2015 году самая продолжительная DDoS-атака продолжалась 13,3 дней [6][1].

Наиболее известные нарушения информационной безопасности компьютерных сетей – сбои, отказы, стихийные бедствия, побочные влияния и ошибки. Смысл этих явлений (кроме стихийных бедствий) выражается следующим образом [7, 8]:

• отказ – сбой в работе какого-либо элемента системы, приводящий к невозможности выполнения им основных своих функций;

• сбой – временное нарушение в работе какоголибо элемента системы, вследствие чего он не может выполнять свои функции;

• ошибка – неправильное (единичное или периодичное) выполнение элементом одной или нескольких функций, происходящее вследствие специфического (постоянного или временного) его состояния;

• побочное влияние – негативное воздействие на отдельные элементы системы или на нее в целом, оказываемое какими-либо явлениями, происходящими во внешней среде или внутри системы.

Самыми неуязвимыми для вирусов и удалённых сетевых атак считались операционные системы Apple, но в последнее время, как показывает статистика, они всё чаще подвергаются атакам вредоносных программ. За первые девять месяцев 2015 года подобных атак на системы Apple было в семь раз больше, чем за весь предыдущий год, а пик заражений пришелся на первый квартал 2015 года. Например, в марте было предпринято более 65 тыс. атак на компьютеры фирмы Apple [9].

Команда экстренного реагирования на киберугрозы промышленных систем управления – ICSCERT, выпустила в США доклад «Incident response/vulnerability coordination in 2014», в котором была приведена статистика инцидентов информационной безопасности в автоматизированных системах управления технологическими процессами (АСУ ТП) и критически важных объектах. В докладе приведен обзор состояния информационной безопасности в АСУ ТП и критически важных объектах. В России пока такая статистика не приводится, хотя в ближайшем будущем планируется создать собственный CERT [11][3].

По итогам 2014 года ICS-CERT получила от владельцев критически важных объектов и отраслевых партнеров информацию о более 200 нарушениях информационной безопасности. Лидером по количеству выявленных нарушений является энергетический сектор. При этом сотрудничество энергетического сектора и CERT дает возможность эффективно реагировать на подобные нарушения [12]. Следует упомянуть, в 2014 году были сообщения об нарушениях в критически важных секторах промышленности, включая АСУ ТП производителей оборудования. Поставщики промышленного оборудования АСУ ТП – одна из главных целей для экономической разведки и шпионажа [12][2].

Около 55 % обнаруженных нарушений приходится на направленные атаки и действия квалифицированных злоумышленников. К другим нарушителям относят: хактивистов, преступные элементы, внутренних нарушителей. В большинстве случаев злоумышленники остаются неизвестными [13]. Распределение нарушений информационной безопасности по секторам промышленности представлено на рисунке 1 [11]. Размер негативного воздействия нарушений (инцидентов) и количество методов воздействия с целью получения несанкционированного доступа к инфраструктуре бизнес-систем и АСУ ТП достаточно широк. На рисунке 2 приведен пример некоторых из них [14].

Распределение нарушений в критически важных объектах и АСУ ТП по векторам атак представлено на рисунке 3 [11].

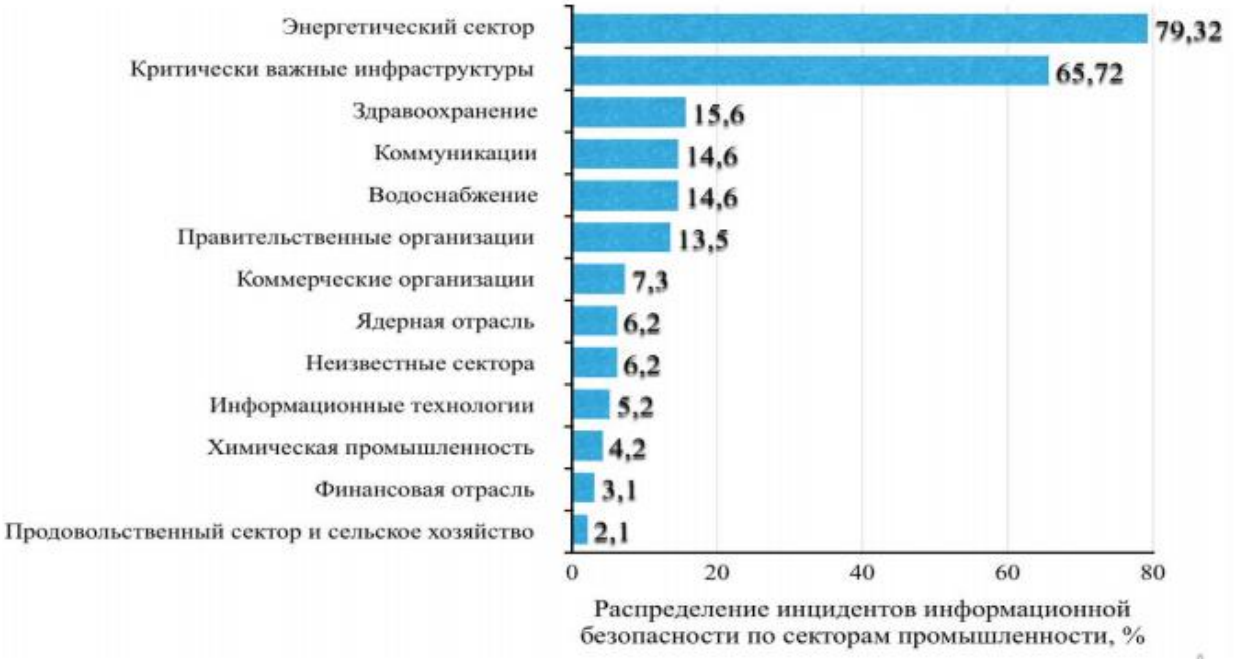

Рисунок 1 – Распределение нарушений информационной безопасности по секторам промышленности

Несанкционированный доступ и эксплуатация внешнего web client-side АСУ ТП или SCADA	Перемещение между сегментами сети	Эксплуатация уязвимостей нулевого дня в контролирующих устройствах и программном обеспечении
Распространение инфекций в беспроводных сетях систем управления	**Инциденты**	SQL инъекции через эксплуатацию уязвимостей веб-приложений
Сканирование и зондирование сети	Атаки на веб-сайты (watering hole)	Таргетированные атаки посредством социальной инженерии в электронной почте

Рисунок 2 – Примеры негативного воздействия нарушений (инцидентов)

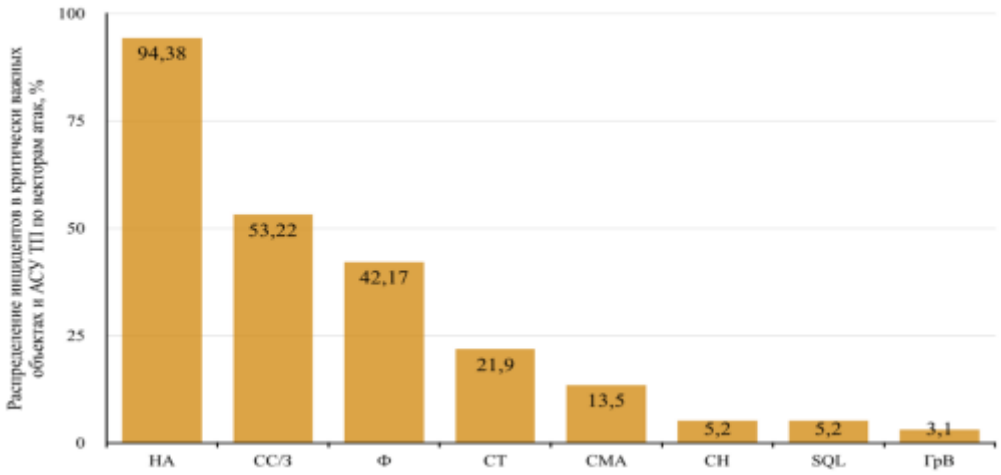

Рисунок 3 – Нарушения в критически важных объектах и АСУ ТП по векторам атак НА – неизвестные атаки, СС/З – сканирование сети/зондирование, Ф – фишинг по e-mail, СТ – смешанные типы, СМА – слабые механические аутентификации, СН – съемные носители, SQL–SQL – инъекции, ГрВ – «грубые» вторжения

На первый взгляд достаточно простыми и наименее финансово-затратными выглядят административные меры обеспечения информационной безопасности сетей предприятия. Основная цель принимаемых мер на административном уровне – разработка программы работ в области улучшения доступности информационных услуг и обеспечение их выполнения, выделяя необходимые ресурсы и контролируя фактическое положение дел [15].

На первом этапе по разработке программы анализируют угрозы и риски.

Средства обеспечения информационной безопасности в зависимости от их реализации разделяют на классы методов (рис. 4) [17].

Типы защиты сети можно разбить на четыре основные категории (рис. 5) [17, 18].

1. Физическая безопасность. Любой компьютер, будь то рабочая станция, сетевой сервер, общественный терминал в уличном киоске или ноутбук, нуждается в обеспечении физической защитой. 2

2.. Безопасность пользователей имеет следующие аспекты:

• возможность предоставления пользователям доступа к информационным ресурсам в соответствии с их потребностями;

• необходимость не предоставлять (а в некоторых случаях скрывать) от пользователей ресурсов ту информацию, которая не требуется им для работы. К такой информации относится важная для компании информация и персональные данные. Контроль доступом заключается во взаимном опознании пользователя и системы и определении степени допустимости использования того или иного ресурса конкретным пользователем в соответствии с его запросом.

3. Защита файлов также имеет некоторые аспекта:

• управление доступом к файлам;

• защита целостности файла. Преступник намеренно вошедший в систему может уничтожить, удалить или изменить информацию в файлах. Поэтому рекомендуется ввести некоторые ограничения на обработку файлов, являющихся носителями важной информации.

4. Защита от несанкционированного входа реализуется с помощью процедур регистрации обращений, идентификации и аутентификации [4][21].

Идентификация и аутентификация могут быть сделаны в ходе работы неоднократно для исключения возможности доступа к системе злоумышленников, выдающих себя за истинного пользователя.

Централизованное администрирование подразумевает, что один человек, группа или отдел осуществляют административное управление всей корпоративной сетью, ресурсами и пользователями. Главным и достаточно серьезным недостатком централизованной схемы является ее недостаточная масштабируемость и отсутствие отказоустойчивости. От производительности центрального компьютера зависит число пользователей, работающих с приложениями, и выход из строя центрального компьютера приведет к нарушению работы всех пользователей [19, 20]. Данную модель хорошо применять в небольших и средних организациях, а для для крупных или территориально распределенных предприятий она может быть неэффективной. Однако, учитывая вопросы безопасности, централизованное администрирование является лучшим. Оно гарантирует единство системной политики и процедур для всей организации [5].

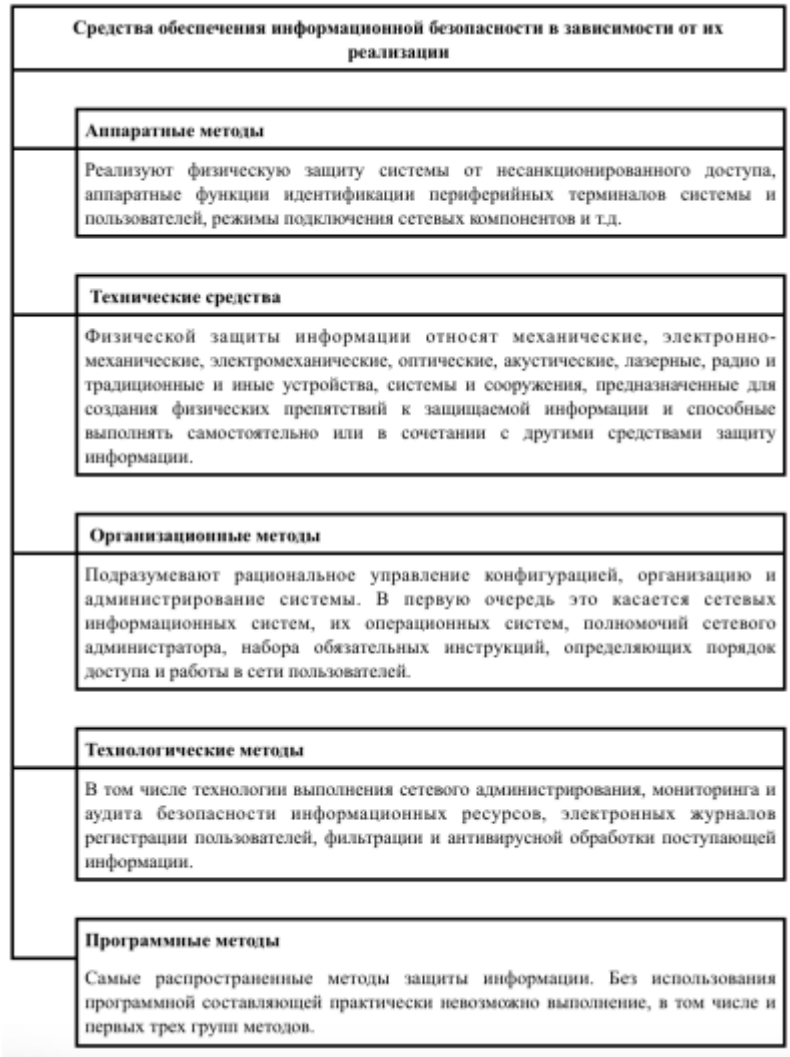

Рисунок 4 – Средства обеспечения информационной безопасности в зависимости от их реализации

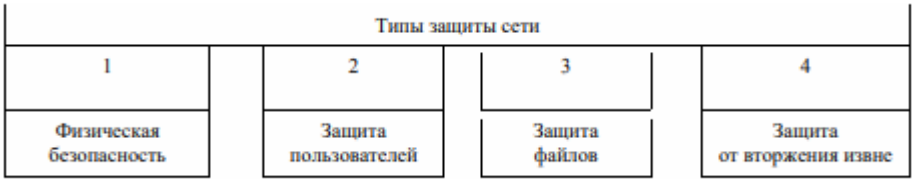

Рисунок 5 – Типы защиты сети

Распределенное администрирование сети подразумевает управление, осуществляющееся на уровне отдела или рабочей группы. Хотя администрирование на этом уровне имеет возможность оперативно реагировать на потребности пользователей, зачастую это достигается за счет сетевой безопасности. Если на предприятии несколько администраторов, политика администрирования в различных рабочих группах будет отличаться. Чем больше число групп, тем больше доверительных отношений, в которых они нуждаются, что повышает вероятность проникновения злоумышленников в систему с целью получения секретной информации, используя доверительные отношения [19, 20].

Администрирование на уровне операционных систем включает в себя средства безопасности существенно различающиеся в зависимости от используемых операционных систем. Например, имеется администратор серверов Windows NT, серверов Novell Net Warel и серверов Unix-систем, каждый из них гарантирует безопасность своей сети. Тем не менее необходим специалист, который будет урегулировать разногласия администраторов в случае возникновения проблем [19, 20].

Смешанная модель администрирования сочетает в себе распределенную и централизованную модели. Центральный администратор (или группа) обеспечивает проведение политики безопасности в масштабах всего предприятия, а администраторы на уровне отделов или рабочих групп выполняют повседневную работу. Это обычно требует больше затрат для содержания штата сотрудников, поэтому использование смешанной модели управления чаще применяется крупными предприятиями [19, 20].

Политика безопасности должна применяться в рамках всей организации.

Несмотря на соответствие самым строгим требованиям безопасности, если система некорректно спроектирована и плохо управляется, то возможна неэффективная защита и сложность использования системы по прямому назначению. Необходимо учитывать, что повышение уровня безопасности системы требует больше времени и административных усилий, чтобы управлять ими.

При построении системы защиты целесообразно придерживаться следующих принципов:

- актуальность, чтобы обезопасить себя от реальных атак, а не от фантастических или архаичных;

- обоснованность расходов, поскольку 100 % защита нереальна, необходимо найти точку, в которой дальнейшие расходы на повышение безопасности будут превышать стоимость информации, которую злоумышленники могут украсть [21].

Список использованных источников:

1. Варфоломеев А. А. Основы информационной безопасности: Учеб. пособие. М. : РУДН, 2008. 412 с.

2. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Том 1. Технические каналы утечки информации. М. : НПЦ «Аналитика», 2008. 436 с.

3. Alan G. Konheim – Computer security and cryptography. Изд-во : John Wiley & Sons, Inc., 2007. 542 с.

4. Артемьева Ю. В. Маркетинговая безопасность? Принцип работы // Маркетинг в России и за рубежом. 2011. № 6. С. 32–38.

5. Ломаков Ю. А. Методики оценивания рисков и их программные реализации в компьютерных сетях // Молодой ученый. 2013. № 2. С. 43–46.

6. DDoS-атаки в третьем квартале 2015 года [Электронный ресурс] URL: https://securelist.ru/files/ 2015/11/Q3_DDoS_report_RUS.pdf (дата обращения: 07.01.2016).

7. Абрамов Н. С., Фраленко В. П. Угрозы безопасности вычислительных комплексов: классификация, источники возникновения и методы противодей- ствия // Программные системы: теория и приложения. 2015. № 6:2 (25). С. 63–83.

8. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации: учебное пособие. М. : Центр ЕАОИ, 2012. 311 с.

9. Число вирусных атак на компьютеры Apple выросло в семь раз [Электронный ресурс] URL: http://itbusiness.com.ua (дата обращения: 09.01.2016).

10. Symantec: количество угроз для OS X и iOS продолжает расти раз [Электронный ресурс] URL: http://club-symantec.ru (дата обращения: 09.01.2016).

11. Статистика инцидентов, угроз и уязвимостей информационной безопасности в КВО и АСУ ТП [Электронный ресурс] URL: https: // tosaithe.wordpress.com (дата обращения: 09.01.2016).

12. Отчёт ICS-CERT за июль-август [Электронный ресурс] URL: http://www.securitylab.ru (дата обращения: 09.01.2016).

13. Синещук Ю. И. Основные угрозы и направления обеспечения безопасности единого информационного пространства / [и др.] // Вестн. С.-Петерб. ун-та МВД России, 2013. № 2. С. 150–154.

14. Алаева С. С., Бобков С. П., Ситанов С. В. Администрирование в информационных системах: учеб. пособие / Иван. гос. хим.-технол. ун-т. Иваново, 2010. 52 с.

15. Крат Ю. Г., Шрамкова И. Г. Основы информационнойбезопасности : учеб. пособие. Хабаровск : Изд-во ДВГУПС, 2008. 112 с.

16. Громов Ю. Ю., Иванова О. Г., Мосягина Н. Г., Набатов К. А. Надёжность информационных систем : учебное пособие / Тамбов : Изд-во ГОУ ВПО ТГТУ, 2010. 160 с.

17. Жигулин Г. П. Организационное и правовое обеспечение информационной безопасности. СПб. : СПб НИУИТМО, 2014. 173 с.

18. ЗавгороднийВ. И. Комплексная защита информации в компьютерных системах: учебное пособие. М. : Логос; ПБОЮЛ Н. А. Егоров, 2001. 264 с.

19. Туккель И. Л. Методы и инструменты управления инновационным развитием промышленных предприятий. СПб. : БХВ-Петербург, 2013. 208 с.

20. Кустов Н. Т. Администрирование информационно-вычислительных сетей : учебное пособие. Томск : Томскийгосударственныйуниверситет, 2004. 247 с.

21. Вишняков В.А. Информационная безопасность в корпоративных системах, электронной коммерции и облачных вычислениях: методы, модели, программно-аппаратные решения – Минск, 2012. – 274 с.: ил. (С.11-21. Раздел 1. Основные проблемы информационной безопасности).