Некрасова Евгения Александровна
заведующая учебно-лабораторным комплексом
Головачев Алексей Алексеевич
магистрант
ФГАОУ ВО «Северо-Кавказский федеральный университет»
г. Ставрополь, Ставропольский край

КЛАССИФИКАЦИЯ УГРОЗ НАРУШЕНИЯ ДОСТУПНОСТИ ИНФОРМАЦИИ И ИСТОЧНИКИ ИХ ВОЗНИКНОВЕНИЯ

Аннотация: *авторы статьи отмечают, что сведения о предполагаемых угрозах и знания уязвимых мест защиты, через которые эти угрозы могут воздействовать, необходимы для выбора экономичных средств обеспечения безопасности.*

Ключевые слова: *атака, угроза, злоумышленник, источник угрозы, окно опасности, уязвимость, программное обеспечение, информационные системы, информация, доступ, субъект информационных отношений, ущерб, размер ущерба, непреднамеренные ошибки.*

Атакой называется попытка реализации угрозы. Угроза – возможное вероятное нарушение информационной безопасности посредством выполнения определенных действий. Субъект, предпринимающий такую попытку, является злоумышленником. Потенциального злоумышленника обычно называют источником угрозы.

В большинстве случаев, угроза выступает как следствие наличия слабых мест в защите информационных систем (например, ошибки в специализированном программном обеспечении или наличие доступа сторонних лиц к важному оборудованию).

Под окном опасности, ассоциированным с уязвимым местом, обычно понимают период времени с момента [1] появления возможности использовать уязвимое место до момента ликвидации такой возможности.

Успешные атаки на систему возможны до тех пор, пока существует такое окно опасности.

При наличии ошибок [2] в программном обеспечении, окно опасности появляется с возникновением средств, использующих ошибки и устраняется в момент исправления этих ошибок.

В большинстве уязвимых мест окно опасности открыто несколько часов, дней, недель, поскольку за такой промежуток времени [3] должны произойти следующие события:

– необходимо выяснить, какие средства используют пробелы в защите;

– необходимо произвести соответствующие заплаты в уязвимых местах;

– установка заплат должна быть произведена в защищаемой системе.

Новые уязвимые места и средства их использования не перестают возникать постоянно. В свою очередь, это означает что:

– почти всегда существуют окна опасности;

– отслеживание таких окон должно производиться постоянно;

– выпуск и наложение заплат должно производиться незамедлительно.

Нельзя не отметить, что некоторые угрозы не всегда считаются следствием каких-то ошибок. Они возникают в силу самой природы современных систем и сетей.

Современные информационные системы подвержены различным угрозам, рассмотрим наиболее распространенные из них. Для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности [4], необходимо иметь знания о возможных угрозах, а также об уязвимых местах, которые эти угрозы обычно используют.

Существование множества мифов в сфере информационных технологий часто приводит к нерациональному использованию и перерасходу ресурсов, а также к средоточию средств там, где они не особенно нужны, за счет ослабления действительно уязвимых направлений.

Стоит подчеркнуть, что понятие «угроза» в различных условиях понимается и объясняется по-разному. Так, например, для открытой организации угроз конфиденциальности [5] может просто не возникать – вся информация считается общедоступной. Однако часто несанкционированный доступ представляет собой серьезную опасность. То есть, угрозы в информационной безопасности зависят от интересов субъектов информационных отношений и от того, какой ущерб для них недопустим.

Классификацию угроз можно провести по следующим критериям:

– по способу осуществления (преднамеренные или случайные, действия техногенного или природного характера);

– по расположению источника угроз (вне или внутри рассматриваемой системы);

– по компонентам информационных систем (поддерживающая инфраструктура, аппаратура, программы, данные), на которые угрозы нацелены;

– по аспекту информационной безопасности [6], на который угрозы направлены в первую очередь (конфиденциальность, целостность, доступность).

Обычно, основным критерием используют четвертый – по аспекту информационной безопасности.

С точки зрения размера ущерба самыми опасными и частыми являются непреднамеренные ошибки штатных сотрудников, операторов, пользователей, системных администраторов и других лиц, которые обслуживают информационные системы.

Такие непреднамеренные ошибки иногда и являются собственно угрозами – например, ошибка в программе или неправильно введенные данные [7], вызвавшие крах системы. Злоумышленники пользуются уязвимыми местами, которые создают эти ошибки. По статистическим данным, до 65 процентов потерь случается из-за непреднамеренных ошибок.

Наводнения, землетрясения и пожары и не приносят такое количество потерь, какое приносит наличие человеческого фактора – безграмотность и небрежность сотрудников в работе.

Таким образом, можно сказать, что самый действенный способ борьбы с непреднамеренными ошибками – максимальная автоматизация [8] и строгий контроль.

Другие угрозы доступности классифицируются по компонентам информационных систем, на которые нацелены угрозы:

– внутренний отказ информационной системы;

– отказ поддерживающей инфраструктуры;

– отказ пользователей.

– Применяемо к пользователям рассматриваются следующие угрозы:

– невозможность выполнения работы с системой из-за отсутствия соответствующей подготовки (общая компьютерная безграмотность, неумение работать с документацией, неумение интерпретировать диагностические сообщения и т. п.);

– невозможность выполнения работы с системой из-за отсутствия технической поддержки (неполнота справочной информации, недостаток документации и т. д.);

– отсутствие желания выполнения работы с информационной системой – чаще всего проявляется с необходимостью освоения новых возможностей, а также с расхождением между запросами пользователей и фактическими возможностями или техническими характеристиками.

К основным источникам внутренних отказов можно отнести:

– случайные или преднамеренные действия пользователей или обслуживающего персонала, приводящие к выходу системы из штатного режима эксплуатации;

– умышленное или случайное отступление от рекомендованных правил эксплуатации;

– возникновение отказов программного и аппаратного обеспечения;

– разрушение данных;

– возникновение ошибок при (пере)конфигурировании системы;

– разрушение или повреждение аппаратуры.

Рекомендуется рассматривать следующие угрозы по отношению к поддерживающей инфраструктуре:

– нежелание или невозможность обслуживающего персонала или пользователей выполнять свои обязанности;

– умышленное или случайное нарушение работы электропитания, систем связи, водо- и теплоснабжения, кондиционирования;

– повреждение или разрушение помещений.

Особенную опасность представляют так называемые «обиженные» сотрудники – как правило, они стремятся нанести вред «организации-обидчику», например:

– повредить, украсть/передать сторонним лицам, удалить данные;

– занести логический вирус, который со временем разрушит программы или данные;

– испортить оборудование.

Такие даже бывшие обиженные сотрудники, хорошо изучили порядки в организации и способны нанести значительный ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа как логического, так и физического к информационным ресурсам аннулировались.

Список литературы

1. Тебуева Ф.Б. Математические модели и методы для задач многокритериального выбора на графах в условиях недетерминированности исходных данных: Автореф. дис. … д-ра физ.-мат. наук. – Ставрополь, 2013. – 35 с.

2. Kopytov V.V. An improved brown's method applying fractal dimension to forecast the load in a computing cluster for short time series / V.V. Kopytov, V.I. Petrenko ., F.B. Tebueva, N.V. Streblianskaia // Indian Journal of Science and Technology. – 2016. – Т. 9 – №19. – С. 93909.

3. Тебуева Ф.Б. Два подхода к реализации фрактального анализа временных рядов // Научно-технические ведомости СПбПУ. Естественные и инженерные науки. – 2007. – №52–2. – С. 105–112.

4. Петренко В.И. Проблемы безопасности автоматизированных систем управления технологическими процессами в России / В.И. Петренко, Д.Н. Суховей // Актуальные проблемы современной науки Международная научно-практическая конференция / Северо-Кавказский гуманитарно-технический институт (Россия); Словацкий университет святых Кирилла и Мефодия (Словакия); Словацкий технологический университет в Братиславе (Словакия); Северо-Кавказский федеральный университет, институт информационных технологий и телекоммуникаций (Россия); Филиал ВНИИ МВД России по СКФО (Россия). – 2013. – С. 185–189.

5. Жук А.П. Совершенствование математического аппарата синтеза ортогональных дискретных последовательностей для широкополосных беспроводных систем связи / А.П. Жук, В.И. Петренко, Ю.В. Кузьминов, Н.С. Дорошенко // Вестник СевКавГТИ. – 2012. – №13. – С. 10–15.

6. Сагдеев К.М. Физические основы защиты информации / К.М. Сагдеев, В.И. Петренко , А.Ф. Чипига. – Ставрополь: Издательство Северо-Кавказского федерального университета, 2015. – 394 с.

7. Некрасова Е.А. Моделирование при системном анализе сложных технических систем // Студенческая наука для развития информационного общества: сборник материалов III Всероссийской научно-технической конференции. – Ставрополь: Изд-во СКФУ, 2015. – 313 с.

8. Сашенко А.С. Гибридные модели в современных инструментах моделирования / А.С. Сашенко, Е.А. Некрасова // Прошлое, настоящее и будущее российской цивилизации: Материалы всероссийской научно-практической конференции. – Ставрополь: Мир данных, 2016. – 112 с.