Алгоритм реагирования на инциденты информационной безопасности в МОУ ИТЛ№24

Сокращения

АЗИ – Межрегиональная общественная организация «Ассоциация защиты информации»;

АРСИБ – Межрегиональная общественная организация «Ассоциация руководителей служб информационной безопасности»;

ДБО – дистанционное банковское обслуживание;

ИБ – информационная безопасность;

НЖМД – накопитель на жёстких магнитных дисках;

ПО – программное обеспечение;

СБ – Служба безопасности;

СИБ – Служба информационной безопасности;

СОДИТ – Межрегиональная общественная организация «Союз ИТ-директоров России»;

ЭЦП – электронная цифровая подпись;

DDoS-атака (от англ. Distributed Denial of Service) – распределенная атака типа «отказ в обслуживании»;

DoS-атака (от англ. Denial of Service) – атака типа «отказ в обслуживании».

Инциденты ИБ и законодательство РФ.

В настоящее время наблюдается значительный рост числа фиксируемых в организациях инцидентов информационной безопасности, имеющих как внутренний, так и внешний характер. Внутренний инцидент – инцидент, источником которого является нарушитель, связанный с пострадавшей стороной непосредственным образом (трудовым договором или иным способом).

Среди системных событий такого типа можно выделить следующие наиболее распространенные:

- утечка конфиденциальной информации;
- неправомерный доступ к информации;
- удаление информации;
- компрометация информации;
- саботаж;
- мошенничество с помощью ИТ;
- аномальная сетевая активность;
- аномальное поведение бизнес-приложений;
- использование активов компании в личных целях или в мошеннических• операциях.

Внешний инцидент – инцидент, источником которого является нарушитель, не связанный с пострадавшей стороной непосредственным образом. Среди системных событий такого типа можно выделить следующие наиболее распространенные:

- мошенничество в системах ДБО;
- атаки типа «отказ в обслуживании» (DoS), в том числе распределенные (DDoS);
- перехват и подмена трафика;
- неправомерное использование корпоративного бренда в сети Интернет;
- фишинг;
- размещение конфиденциальной/провокационной информации в сети Интернет, взлом, попытка взлома, сканирование портала компании;
- сканирование сети, попытка взлома сетевых узлов;
- вирусные атаки;
- неправомерный доступ к конфиденциальной информации;
- анонимные письма (письма с угрозами).

Зачастую действия компьютерных злоумышленников вступают в противоречие с действующим уголовным законодательством и посягают на охраняемые уголовным законом общественные отношения. При этом важно отметить, что только правоохранительные или судебные органы могут квалифицировать инцидент ИБ в качестве преступления в сфере компьютерной информации. В главе 28 УК РФ закреплены квалифицирующие признаки компьютерных преступлений и прописаны соответствующие санкции.

На данный момент глава состоит из трех статей:

- *статья 272 УК РФ* «Неправомерный доступ к компьютерной информации». Максимальные санкции – штраф 300 000 рублей или лишение свободы до 5 лет;
- *Статья 273 УК РФ* «Создание, использование и распространение вредоносных• программ для ЭВМ». Максимальные санкции – лишение свободы до 7 лет;
- Статья 274 УК РФ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их• сети». Максимальные санкции – лишение свободы до 4 лет.

Помимо самостоятельного регулирования главой 28 преступлений в сфере компьютерной информации в ряде случаев правоохранительными и судебными органами перечисленные выше статьи используются в совокупности с другими статьями УК РФ. Например, мошенничество в сети Интернет регулируется следующим образом. Ответственность за его совершение регулируется статьей 159 УК РФ «Мошенничество». Данный состав преступления имеет ряд квалифицирующих признаков, но при этом специального квалифицирующего признака – совершенное в сети Интернет – не имеет. Совершение мошенничества в сети Интернет, например мошенничества в системе дистанционного банковского обслуживания (ДБО), в соответствии с действующим уголовным законодательством квалифицируется правоохранительными органами по статье 159 УК РФ в совокупности со статьями 272 и (или) 273 УК РФ. Совокупное применение данных статей действенно при привлечении злоумышленников к уголовной ответственности. Вместе с тем продолжают иметь место проблемы, связанные с уголовным законодательством, при квалификации других видов преступлений, совершенных в сети Интернет: пробелы в уголовном праве в части определения используемых в диспозиции статей главы 28 УК РФ понятий; отсутствие в составах преступлений дополнительных квалифицирующих признаков, из-за чего ряд новых видов преступлений в сфере компьютерной информации не подлежит специальной квалификации, а подгоняется под имеющиеся квалификационные признаки; применение в некоторых случаях статей главы 28 УК РФ с использованием расширенной и необоснованной трактовки квалифицирующих признаков; наличие в уголовном законодательстве «нерабочей» статьи 274 УК РФ. Основным путем решения упомянутых проблем является внесение изменений в действующее законодательство. В настоящее время Комиссия по информационной безопасности и киберпреступности РАЭК, в состав которой входят отраслевые эксперты, осуществляет подготовку предложений о внесении изменений в некоторые законодательные акты Российской Федерации в целях оптимизации борьбы с преступлениями в сфере компьютерной информации, предполагающих в том числе уголовную ответственность за незаконное распространение электронных сообщений (спам). Данные изменения направлены на расширение квалифицирующих признаков в области преступлений в сфере компьютерной информации и ужесточение действующих санкций, что позволит дать эффективный ответ на существующие киберугрозы.

Реагирование на инцидент ИБ

Реагирование на инцидент ИБ включает в себя технические мероприятия, обеспечивающие целостность криминалистически значимых данных и возможность судебного исследования этих данных в будущем, а также организационные мероприятия, которые позволяют снизить ущерб от инцидента и составить необходимые для правоохранительных органов документы. Сущностью технических мероприятий является немедленное обеспечение целостности данных, потенциально имеющих отношение к инциденту, путем отключения, упаковки и опечатывания, а затем и должного хранения соответствующих носителей информации. Отключение носителей информации позволяет свести к нулю риск уничтожения криминалистически значимых данных в результате работы вредоносных программ и действий злоумышленника, а их упаковка, опечатывание и должное хранение обеспечивают достаточный уровень оцениваемой достоверности результатов криминалистического исследования в суде. Организационные мероприятия заключаются в уведомлении руководства организации, подразделений (служб) информационной безопасности организации и иных заинтересованных организаций о факте инцидента. Документы, составленные при проведении организационных мероприятий, могут использоваться как основания для рассмотрения вопросов о возбуждении уголовных дел или для уточнения вопросов, выносимых на разрешение при назначении судебных экспертиз носителей информации организации. После реагирования на инцидент ИБ начинается расследование инцидента и восстановление информационной системы организации. Восстановление информационной системы организации заключается в замене изъятых, упакованных и опечатанных носителей информации на новые, установке требуемого ПО и конфигурации информационной системы с учетом повышенных требований ИБ.

Общий алгоритм действий при наступлении инцидента Основная задача службы ИБ – это предотвращение реализации возможных рисков, связанных с утечкой или потерей информации для компании, которая основана на понимании, формулировании и удовлетворении осознанных пожеланий бизнеса. Деятельность компании в области ИБ описывается в документе «Политика ИБ», где прописаны все общие принципы и правила, а также формализованы задачи на текущий горизонт планирования в компании. В приложении к данному документу необходимо четко и пошагово прописать общий алгоритм действий сотрудников СБ в случае наступления инцидента информационной безопасности.

Типовой сценарий при нарушениях ИБ может быть основан на приведенных ниже базовых действиях.

В случае возникновения инцидента ИБ необходимо:

1. Идентифицировать инцидент и убедиться, что он действительно имеет место быть.
2. Локализовать область ИТ-инфраструктуры, задействованной в инциденте.
3. Ограничить доступ к объектам, задействованным в инциденте.
4. Оформить служебную записку на имя Генерального директора организации о факте возникновения инцидента.

5. Привлечь компетентных специалистов для консультации.

6. Создать группу по расследованию инцидента и составить план работ по сбору доказательств и восстановлению систем. Протоколировать все действия, которые осуществляются в ходе реагирования на инцидент.

7. Обеспечить сохранность и должное оформление доказательств.

7.1. Снять энергозависимую информацию с работающей системы.

7.2. Собрать информацию о протекающем в реальном времени инциденте.

7.3. Отключить от сети питание.

8. В присутствии третьей независимой стороны произвести изъятие и опечатывание носителей информации с доказательной базой, а также снятие образов и другой информации для последующего анализа и сохранения.

8.1. Оформить протоколом все операции с носителями информации.

8.2. Провести детальную опись объектов с информацией, извлекаемых данных, а также мест их сохранения.

8.3. Задокументировать процесс на фото-видеокамеру.

8.4. Сохранить опечатанные объекты вместе с протоколом в надежном месте до передачи носителей на исследование или в правоохранительные органы.

9. После сохранения и оформления вещественных доказательств восстановить работоспособность информационных систем.

10. При проведении исследования источников информации обеспечить неизменность доказательств. Работать только с копией.

11. При проведении расследования обеспечить корректное взаимодействие с заинтересованными подразделениями (Управление «К», Центр информационной безопасности ФСБ РФ) и внешними организациями (компании, предоставляющие услуги в области расследования инцидентов ИБ и обеспечения ИБ).

12. По завершении расследования оформить соответствующий отчет и составить рекомендации по снижению рисков возникновения подобных инцидентов в будущем.

13. При обращении в правоохранительные органы представить им подробное описание инцидента, описание собранных доказательств и результаты их анализа.

Алгоритм реагирования на инциденты информационной безопасности

Разработано: Директор Жилин С.М.

Заместитель директора по безопасности Белов Е.Ю.