Тема: Современные факторы, влияющие на защиту информации

2020

Тема: Современные факторы, влияющие на защиту информации

Учебные вопросы:

1. Уязвимость информации
2. Формы и причины проявления уязвимости информации
3. Понятие, причины и условия утечки защищаемой информации.

Литература

Основная:

1. В.И. Ярочкин Информационная безопасность. – М.: Гаудеамус, 2004. – 544с.

.В.В. Мельников, С.А. Клейменов, А.М. Петраков Информационная безопасность. – М.: Академия, 2005. – 336с.

.В.В. Мельников Безопасность информации в автоматизированных системах. – М.: Финансы и статистика, 2003. – 368с.

.В.А. Герасименко, А.А. Малюк Основы защиты информации. – М.: 2000.

Литература

Дополнительная:

5. П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков Теоретические основы компьютерной безопасности: Учебное пособие для ВУЗов. – М.: Радио и связь, 2000. – 192с.

6. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: Учебник/ Под ред. Акад. РАН Б.Н. Топорникова. - СПб.: Издательство «Юридический центр Пресс», 2001.

.Информатика и вычислительная техника в деятельности органов внутренних дел. Учебное пособие в 6-ти частях. Под ред. В.А. Минаева. М.: МЦПО и КНИ при ГУК МВД России. 1995, 1996.

8. Копылов В.А. Информационное право. Учебное пособие. М., 1997.

.Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. М., 1998.

Введение

Факторы, влияющие на защиту информации, обусловлены объективными тенденциями развития мирового сообщества, характер их влияния на защиту информации определяется экономическими, политическими и социальными процессами, протекающими в различных сферах человеческой деятельности в государственных, частных и общественных структурах.

Факторы, обусловленные современным состоянием России. Влияние политико-правовых и социально-экономических реальностей, реальностей борьбы с преступностью на защиту информации

1. Уязвимость информации

Информация как объект информационного процесса и как объект защиты имеет ряд свойств. Наиболее важными для информации, особенно для защищаемой, являются такие ее свойства, как конфиденциальность, целостность, доступность, а также ценность, полезность, истинность. Эти свойства информации не являются постоянными величинами, поскольку существуют различные виды угроз, которые направляют свои действия на полное или частичное разрушение этих свойств.

Свойство уязвимости означает неспособность информации самостоятельно противостоять дестабилизирующим воздействиям, сохранять при таких воздействиях свой статус. В целом термин "уязвимый" означает слабый, мало защищенный. Следовательно, уязвимость представляет собой такую характеристику, которая делает объект слабым и мало защищенным.

Уязвимость информации, в свою очередь, является характеристикой, которая делает возможным в результате определенных причин возникновение и/или реализацию угрозы или группы угроз, направленных на информацию, отдельные свойства информации, а также на носитель информации.

Угроза информации – это совокупность условий и фактов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности информации.

Угрозы конфиденциальности информации направлены на несанкционированное перемещение информации от носителя-источника к носителю-получателю (угроза разглашения, утечки, несанкционированного доступа).

Угрозы целостности информации направлены на несанкционированное изменение или искажение защищаемой информации, приводящие к нарушению ее качества или полному уничтожению (угроза искажения, ошибки, потери).

1. Уязвимость информации

Угрозы доступности информации (отказ в обслуживании) направлены на преднамеренное или непреднамеренное нарушение коммуникативности носителей информации при их взаимодействии (угроза фальсификации, подделки, мошенничества). Нарушение коммуникативности прерывает разрешенные режимом доступа процессы перемещения информации. Коммуникативность – совместимость, способность к совместной работе разнотипных систем передачи информации.

Виды уязвимости информации.

Виды уязвимости информации можно выделить в зависимости от угроз, к которым они тяготеют. Для каждой существующей угрозы информации существует, в свою очередь, уязвимость, которая позволяет эту угрозу реализовать в меньшей или большей степени. Выделяют три основных вида угроз информации: *утечка*, *НСД*, *разглашение*.

Эти угрозы создают предпосылки для следующих видов уязвимости информации:

1. *Уязвимость информации к стихийным бедствиям* определяется наличием у информации или у ее носителя свойств, которые делают возможным утечку, несанкционированные получение, модификацию, уничтожение информации, блокирование доступа к ней в результате природных катаклизмов (землетрясение, на-

1. Уязвимость информации

2. *Уязвимость информации к непреднамеренным* (случайным, неосторожным) действиям сотрудников или иных лиц обусловлена недостаточной защищенностью информации от определенных действий человека (сотрудника или иного лица), совершаемых из-за его неопытности, неосторожности, несоблюдения установленных требований по охране труда и выполнению определенных работ, неправильной организации работы с носителями информации, случайных ошибок, сбоя технических или программных средств и других нецеленаправленных действий.

3. *Уязвимость информации к преднамеренным действиям злоумышленников или иных заинтересованных лиц* является наиболее опасной. Как уже отмечалось выше, различные виды уязвимости обусловлены угрозами разглашения, НСД и утечки информации.

1. *Уязвимость информации к разглашению* – несанкционированному сообщению защищаемой информации лицам, не имеющим права доступа к ней, – определяется, прежде всего, неправильной организацией работы с информацией и ее носителями, а также неосторожными или умышленными действиями людей, допущенных к работе с данной

информацией.

2. *Уязвимость информации к НСД* – противоправному преднамеренному овладению защищаемой информацией лицом, не имеющим права доступа к ней, – определяется наличием у информации, ее носителя или у самой системы защиты недостатков, которые

1. Уязвимость информации

3.3. *Уязвимость информации к утечке* – неконтролируемому распространению защищаемой информации за пределы круга лиц, которым эта информация была доверена, – возникает, как и в случае разглашения, из-за неправильной организации работы с информацией, а также в связи с "дырами" в системе защиты информации, неосторожными или умышленными действиями людей, допущенных к работе с защищаемыми сведениями.

Уязвимость по времени действия угроз может быть:

- *постоянной* – уязвимость, которая существует очень длительный промежуток времени, пока действует текущая система защиты информации, при несовершенстве которой эта уязвимость и возникла;
- *периодической* – уязвимость, которая возникает периодически при определенных обстоятельствах или действиях со стороны человека, при регулярном нарушении определенных правил работы с информацией, несоблюдении требований к организации системы защиты информации;
- *разовой* – уязвимость, которая носит случайный характер и возникает обычно из-за ошибок персонала.

2 Формы и причины проявления уязвимости информации

Уязвимость информации – понятие собирательное, она не существует сама по себе, а проявляется (выражается) в различных формах. Наличие уязвимости информации определяется по фактам различных форм проявления уязвимости, которые указывают собственнику (владельцу или пользователю) информации, куда, прежде всего, будет направлен основной удар злоумышленника, если тот поставит себе цель получить, модифицировать, уничтожить информацию или блокировать доступ к ней.

К формам проявления уязвимости информации, выражающим результаты дестабилизирующего воздействия на информацию, должны быть отнесены:

- хищение носителя информации или отображенной в нем информации (кража);
- потеря носителя информации (утеря);
- несанкционированное уничтожение носителя информации или отображенной в нем информации (разрушение);
- искажение информации (несанкционированное изменение, несанкционированная модификация, подделка, фальсификация);
- блокирование информации;
- разглашение информации (несанкционированное распространение, раскрытие).

О*сновные причины возникновения у информации свойства уязвимости*:

- несовершенство или нарушение организации работы с информацией или носителем информации;
- несовершенство системы защиты информации или нарушения в обеспечении информационной безопасности;
- негативные социальные и психологические явления, происходящие в организации или структурном подразделении организации;

2 Формы и причины проявления уязвимости информации

1.Несовершенство или нарушения организации работы с информацией или с носителем информации.

При организации работы с информацией (носителем информации) необходимо учитывать следующие факторы:

доступность информации для сотрудников организации (если эта информация не является конфиденциальной);

оперативность движения информации;

создание условий для оперативного использования информации;

возможность оперативного поиска информации;

выбор рациональной технологии работы с информацией;

рациональная организация рабочих мест и условий труда сотрудников;

выбор оптимальной организационной формы работы с информацией (централизованная, децентрализованная, смешанная);

разработка и внедрение нормативных и методических документов по организации работы с информацией и другие.

2. Несовершенство системы защиты информации или нарушения в обеспечении информационной безопасности.

Несовершенство системы защиты информации (СЗИ) может проявляться в следующих условиях:

- действия СЗИ охватывают не всю систему информационной деятельности, или же имеются плохо защищенные элементы этой системы;
- защита информации не является непрерывной в пространстве и во времени;

2 Формы и причины проявления уязвимости информации

2.3 Негативные социальные и психологические явления, происходящие в организации или ее структурном подразделении.

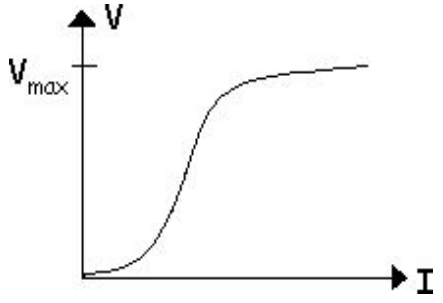
Негативные социальные и психологические явления, происходящие в организации или ее структурном подразделении, включают в себя:

- слабую воспитательно-профилактическую работу в коллективе и недостаточное внимание руководства организации к проблемам или достижениям сотрудников;
- недовольство сотрудников своим материальным обеспечением (низкая заработная плата, отсутствие или низкий размер премии, отсутствие жилья и другие);
- конфликты между сотрудниками, между руководством и подчиненными;
- напряженную психологическую обстановку в коллективе (недоверие, зависть, постоянные стрессовые ситуации, недовольство руководства относительно деятельности того или иного сотрудника, давление и другие);
- невозможность карьерного роста, самореализации, проявления инициативы и другие.

2.4 Высокая ценность информации

Ценность информации определяет ее полезность для собственника или владельца. Она зависит от многих факторов: от количества, качества, достоверности информации, ее способности к старению.

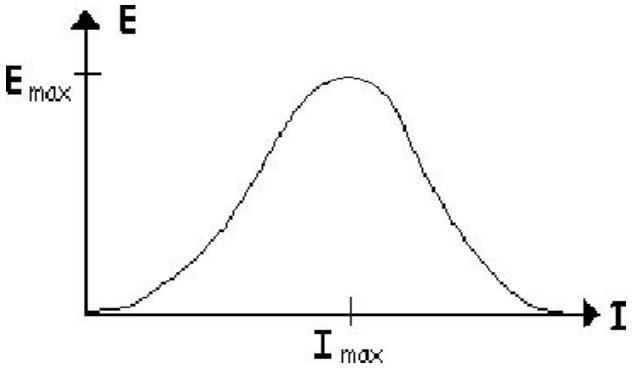
Зависимость ценности информации (V) от ее количества (I):



2 Формы и причины проявления уязвимости информации

2.4 Высокая ценность информации

Зависимость эффективности (E) информации от ее количества (I):



Для оценки количества информации применяется предложенный К. Шенноном термин "энтропия", который означает степень (меру) неопределенности ситуации при условии, что число исходов ее конечно. Энтропия рассчитывается по формуле: $E = -k\sum_{1}^{n} p_i \log p$

где: k – коэффициент, учитывающий выбранное основание логарифма,

p_i – вероятность i-го исхода, n – общее число исходов.

Ценность информации включает в себя и понятие *качества информации*, которое определяется существованием иерархической структуры информации.

Достоверность информации оказывает значительное влияние на ценность информации. Снижение достоверности информации может произойти на любом этапе работы с ней, а также при создании информации (ошибки при вводе информации на носитель, сбои в работе технических средств при приеме поступающей информации, ошибки в программном обеспечении и другие).

2 Формы и причины проявления уязвимости информации

2.5 Уязвимость и информационный риск.

Информационный риск – это возможность реализации потенциальной уязвимости, которая приведет к реализации угрозы. Оценка же информационного риска представляет собой оценку такой возможности.

Анализ информационного риска позволяет одновременно определить имеющиеся уязвимости информации (или информационной системы). Уязвимость информации и информационный риск взаимосвязаны и взаимозависимы друг от друга: уязвимость порождает риск.

В простейшем случае для оценки риска можно использовать два фактора – вероятность происшествия (инцидента) и тяжесть возможных последствий (ущерб от реализации угрозы). Риск тем выше, чем больше вероятность происшествия и тяжесть последствий. В этом случае риск определяется по формуле:

Риск = Вероятность происшествия x Цена потерь

В методиках оценки информационного риска, рассчитанных на более высокие требования, используется модель оценки риска по трем факторам – угроза, уязвимость, цена потери. При этом вероятность происшествия (как объективной, так и субъективной) зависит от вероятности реализации угроз и уровня уязвимости:

Вероятность происшествия = Вероятность угрозы x Уровень уязвимости

Соответственно, риск определяется следующим образом:

Риск = Вероятность угрозы x Уровень уязвимости x Цена потери

2 Формы и причины проявления уязвимости информации

2.5 Уязвимость и информационный риск.

Таблица 1. Определение показателя уровня риска

Тяжесть последствий происшествия (цена потери)	Уровень угрозы								
	низкий			средний			высокий		
	Уровень уязвимости								
	низкий	средний	высокий	низкий	средний	высокий	низкий	средний	высокий
Незначительная	0	1	2	1	2	3	2	3	4
Малая	1	2	3	2	3	4	3	4	5
Умеренная	2	3	4	3	4	5	4	5	6
Серьезная	3	4	5	4	5	6	5	6	7
Критическая	4	5	6	5	6	7	6	7	8

Информационно-аналитическую деятельность по оценке рисков организации может осуществлять как ее служба безопасности, так и специальные информационно-аналитические службы. Результаты информационно-аналитической работы показывают степень безопасности информационных ресурсов и условий функционирования
организации, они являются основой для построения и совершенствования системы защиты информации, позволяют выработать способы активного и пассивного противодействия злоумышленникам.

3.Понятие, причины и условия утечки защищаемой информации

Термин **"утечка информации"** закрепился в научной литературе и нормативных документах, однако единого подхода к определению этого термина нет. Наиболее распространенные определения в обобщенном виде сводятся либо к неправомерному (неконтролируемому) выходу конфиденциальной информации за пределы организаций и круга лиц, которым эта информация доверена, либо к несанкционированному завладению конфиденциальной информацией соперником.

Первый вариант не раскрывает в полной мере сущности утечки, так как он не принимает во внимание последствий неправомерного выхода конфиденциальной информации.

Второй вариант связывает утечку информации с неправомерным завладением конфиденциальной информацией только соперником.

УТЕЧКА ИНФОРМАЦИИ – это неправомерный выход конфиденциальной информации за пределы защищаемой зоны ее функционирования или установленного круга лиц, результатом которого является получение информации лицами, не имеющими к ней санкционированного доступа.

Разглашение защищаемой информации – это несанкционированное ознакомление с такой информацией лиц, не имеющих законного доступа к ней, осуществленное лицом, которому эти сведения были доверены или стали известны по службе.

Раскрытие защищаемой информации – это опубликование ее в средствах массовой информации, использование в выступлениях на публичных конференциях или симпозиумах лицами, которым эти сведения стали известны по службе.

3.Понятие, причины и условия утечки защищаемой информации

Распространение защищаемой информации – это открытоеиспользование сведений ограниченного распространения.

Несанкционированный доступ – получение в обход системы защиты с помощью программных, технических и других средств, а также в силу сложившихся случайных обстоятельств доступа к защищаемой информации.

И сточник утечки защищаемой информации – это любой носитель секретной информации, к которому сумел получить несанкционированный доступ соперник, располагающий необходимыми знаниями и техническими средствами для "снятия", извлечения ин- формации с носителя, ее расшифровки и использования в своих целях в ущерб интересам собственника информации.

Канал утечки защищаемой информации – это социальное явление, отражающее противостояние защитника (собственника) информации и его соперников. В зависимости от используемых соперником сил и средств для получения несанкционированного доступа к носителям защищаемой информации различают агентурные, технические, легальные и иные каналы утечки информации.

3.Понятие, причины и условия утечки защищаемой информации

Агентурные каналы утечки информации – это использование противником тайных агентов для получения несанкционированного доступа к защищаемой информации. *Технические каналы утечки информации* – это совокупность технических средств разведки, демаскирующих признаков объекта защиты и сигналов, несущих информацию об этих признаках.

Легальные каналы утечки информации – это использование соперником открытых источников информации, выведывание под благовидным предлогом сведений у лиц, которым они доверены по службе.

Иными каналами утечки информации являются добровольная (инициативная) выдача сопернику защищаемой информации, экспортные поставки секретной продукции за рубеж и т.п.

Заключение

Утрата и утечка информации могут рассматриваться как виды уязвимости информации.

Формы проявления уязвимости информации выражают результаты конкретного дестабилизирующего воздействия на информацию, а виды уязвимости – конечный суммарный итог реализации различных форм уязвимости.

Утрата информации включает в себя, по сравнению с утечкой, большее число форм проявления уязвимости информации, но она не поглощает утечку, так как не все формы проявления уязвимости информации, которые приводят или могут привести к утечке, совпадают с формами, приводящими к утрате. Если к утрате информации приводит хищение носителей, то к утечке может привести не только хищение носителей, но и копирование, разглашение отображенной в них информации.