

Софтуерно пиратство

Политики за сигурност и правни аспекти при компрометирана система

Софтуерът се използва в образованието, бизнеса, администрацията и личния живот. Правомерното използване изисква спазване на авторските права и приложимите лицензионни условия. Произходът на програмите има значение и за сигурността на системата.

В този урок ще разграничавате формите на софтуерно пиратство, ще предлагате политики за защита на софтуерна система и ще обяснявате действията при компрометиране и нарушаване на сигурността на личните данни.

1 Същност и форми на софтуерно пиратство

Софтуерно пиратство е неправомерно копиране, разпространение, изменение, продажба или използване на софтуер в нарушение на авторските права. Разрешено от носителя на правата или от закона действие не е пиратство. Свободният и безплатният софтуер също имат условия за използване.

Игрите са софтуерни продукти. Неправомерното разпространение на музика и филми също е пиратство, но се отнася до други видове произведения.

Форма	Пример
Неразрешено многократно инсталиране	Лиценз за едно устройство се използва на повече устройства, отколкото допуска.
Зареждане върху продавани компютри	Търговец продава компютри с програми, за които не е осигурено право за ползване.
Фалшифициране	Копия и опаковки се представят за оригинален лицензиран продукт.
Онлайн пиратство	Неразрешени копия се разпространяват чрез сайт, файлов обмен или друг канал.
Заобикаляне на защиты	Използват се неправомерни средства за заобикаляне на активация или лицензиране.

Технологията за обмен, например peer-to-peer, не е незаконна сама по себе си. Важни са съдържанието, разрешението и извършеното действие. Копиране на програма с GPL при спазване на условията е различно от копиране на продукт без право за разпространение.

2 Лицензионно споразумение и последици

EULA (End User License Agreement) е споразумение с краен потребител. Определя разрешенията и ограниченията: брой устройства или потребители, копиране, промени, прехвърляне и условия за поддръжка. Лицензът не забранява непременно всяко копиране. Не всяко договорно нарушение е автоматично нарушение на авторското право; преценява се конкретното действие.

Възможни последици са правна отговорност, разходи за отстраняване на проблеми, загуба на данни и по-висок риск от зловредни добавки. Поддръжката и актуализациите

могат да са ограничени или несигурни. Лицензираният софтуер не гарантира абсолютна безопасност; важни са официалният източник и поддръжката.

BSA (Business Software Alliance) обединява софтуерни компании и работи за спазване на лицензите, управление на софтуерните активи и информираност за рисковете. Това е браншова организация, а не съд или държавен контролен орган.

Допълнителна статия: <https://antivirus.bg/news/софтуерно-пиратство/>.

3 Компрометирана компютърна система

Компрометирана система (compromised system) е система с нарушена сигурност. Нарушението може да засегне данни, акаунти, услуги или управлението на системата. То не се свежда само до видимо проникване на чуждо лице.

Признаци могат да бъдат непознати влизания, неочаквана смяна на настройки, подозрителни съобщения от собствения акаунт, необичайни процеси, криптирани файлове или аларма от защитна програма. Един признак не е окончателно доказателство: забавянето може да има и техническа причина. Случаят се проверява и документира.

Основни цели на сигурността

Цел	Какво се осигурява	Пример за нарушение
Поверителност	Достъп само за оправомощени лица.	Списък с лични данни е видим за всеки.
Цялост	Защита от неправомерна промяна или унищожаване.	Чуждо лице изменя данните.
Наличност	Достъп до информацията и услугите, когато е необходим.	Атака блокира работата на системата.

4 Политики за сигурност на софтуерна система

Политиката за сигурност е набор от цели, правила, отговорности и мерки за опазване на системата и информацията. Тя определя кой има достъп, какво може да прави, как се пазят данните и как се реагира при инцидент. Правилото е конкретно изискване, чрез което политиката се прилага.

Област на политиката	Примерни правила и мерки
Услуги и поддръжка	Разрешен софтуер от проверен източник; актуализации; определени отговорници; резервни копия и проверка на възстановяването; физическа защита.
Мрежова среда	Мрежови правила и защитна стена; защита на отдалечения достъп; контрол на споделените ресурси и изключенията.
Потребители и права	Лични акаунти; минимално необходим достъп; двуфакторна автентикация; заключване при отсъствие; преглед и отнемане на ненужни права.
Лични данни	Ясна цел и основание; минимален набор данни; срок за съхранение; ограничен достъп; ред за искания и сигнали.

Инциденти	Канал за уведомяване; документиране; ограничаване на последиците; възстановяване и проверка; оценка на необходимите външни уведомления.
-----------	---

Удостоверяването проверява самоличността; контролът на достъпа определя позволените действия. Криптиране, резервни копия и мрежово филтриране имат различни цели. Техническото им използване е разгледано в урока „Сигурност и архивиране на данни“; тук се определя кога, от кого и по какви правила се прилагат.

Пример: за училищен проект учениците редактират своите файлове, учителят преглежда всички разработки, а публично се показват само одобрените материали. **Правило „всеки вижда всичко“ не е подходяща политика за лични данни.**

5 Защита на личните данни

Лични данни са сведения за идентифицирано или подлежащо на идентифициране физическо лице. Примери са име, ЕГН, адрес, снимка или онлайн идентификатор, когато позволяват разпознаване. Обработване е събиране, записване, използване, предоставяне, съхраняване или изтриване.

В ЕС основната рамка е Общият регламент относно защитата на данните (ОПЗД, GDPR), Регламент (ЕС) 2016/679. В България се прилага и Законът за защита на личните данни (ЗЗЛД). Надзорният орган е Комисията за защита на личните данни (КЗЛД). GDPR е регламент, а не директива или български закон.

Принципи на обработване

- **Законосъобразност, добросъвестност и прозрачност** — има правно основание и лицето получава ясна информация.
- **Ограничение на целите** — данните се събират за определени допустими цели.
- **Свеждане на данните до минимум** — събира се необходимото за целта.
- **Точност** — неточните данни се коригират.
- **Ограничение на съхранението** — определят се обосновани срокове.
- **Цялост и поверителност** — прилагат се подходящи мерки за сигурност.
- **Отчетност** — администраторът отговаря и може да покаже спазването на изискванията.

Съгласието е едно от възможните основания, но не е единственото. Възможни са например договор или законово задължение. Не се събират данни „за всеки случай“. Снимка с СС лиценз може едновременно да съдържа лични данни — лицензът не отменя изискванията за тяхната защита.

Основни права на физическите лица

Право	Смисъл
Информираност и достъп	Информация за обработването и достъп до собствените лични данни.
Коригиране	Поправка на неточни или допълване на непълни данни.
Изтриване	Искане за заличаване при приложимите условия — „право да бъдеш забравен“.
Ограничаване и възражение	Ограничаване на обработването или възражение в предвидените случаи.
Преносимост	Получаване и прехвърляне на данни в приложимите случаи.
Защита при автоматизирани решения	Гаранции при решения само чрез автоматизирано обработване със съществени последици.
Жалба	Обръщане към надзорния орган при предполагаемо нарушение.

Правата се упражняват при законовите условия. Изтриването не е безусловно, например ако закон изисква съхранение. Правото на достъп до собствените данни не дава право за четене или редактиране на данните на други потребители.

6 Действия при компрометиране и правни последици

Реакция на потребителя

1. Прекратете подозрителното действие и уведомете учителя или отговорния администратор по определения канал.
2. Запишете кога е забелязан проблемът, точния текст и извършеното действие. Не препращайте подозрителния файл на съученици.
3. Следвайте указанията за ограничаване на инцидента. При съмнение за активна атака може да е необходимо отделяне на устройството от мрежата.
4. Не изтривайте произволно файлове и не преинсталирайте с цел „почистване“, преди да е преценено как да се запазят нужните следи.
5. При засегнат акаунт следвайте указанията за смяна на парола и прекратяване на чужди сесии от доверено устройство.

Действия на организацията

Отговорните лица установяват засегнатите системи, данни и потребители, ограничават достъпа и запазват необходимите доказателства. Проверяват причината, отстраняват я, възстановяват от проверено копие и оценяват резултата. Документират инцидента и подобряват политиката, за да се намали повторението.

Нарушение на сигурността на личните данни може да е загуба, неправомерно изменение или неразрешено разкриване и достъп. Ако има вероятност за риск за правата и свободите на лицата, администраторът на лични данни уведомява надзорния орган без ненужно забавяне и, когато е осъществимо, до 72 часа след узнаването. При малко вероятен риск има изключение от уведомяването, но нарушението се документира.

При вероятен висок риск се уведомяват и засегнатите лица без ненужно забавяне, освен при приложимо законово изключение. Уведомлението до органа не е същото като жалба от засегнат гражданин. Обработващият лични данни уведомява администратора без ненужно забавяне. Това са отговорности на организацията, а не задача на ученика да решава сам за уведомяване на КЗЛД.

Отговорност и защита на правата

Според случая могат да възникнат административни санкции, гражданска отговорност и задължение за обезщетение, а при състав на престъпление — наказателна отговорност. Жалба може да се подаде до КЗЛД по установения ред; съдебната защита и обезщетението се разглеждат отделно. Наличието на инцидент само по себе си не определя автоматично санкцията или размера ѝ.

При разкриване на търговска тайна притежателят може да търси защита по ЗЗТТ при изпълнени условия. Авторското право, търговската тайна и личните данни са различни правни режими и един инцидент може да засегне повече от един от тях.

Пример

Публикуван е файл със списък на участници и телефони. Нужно е да се ограничи достъпът, да се установи кои данни и лица са засегнати, да се документира случаят и да се оцени рискът и задължението за уведомяване. Изтриването на публичния файл е мярка, но не доказва, че не са направени копия.

7 Практически задачи

Задача 1 Лиценз и допустимо използване

Разгледайте условията на избрана програма от официалния ѝ сайт. Запишете разрешените устройства или потребители, копиране, промени и разпространение. Сравнете разрешено копиране на свободен софтуер с инсталиране извън разрешения брой устройства.

Задача 2 Политика за учебен проект

Екип пази разработки и работи от различни компютри. Създайте таблица „Риск — правило — отговорник — проверка“. Включете разрешен софтуер, права за четене и редактиране, актуализации, резервно съхранение, лични данни и сигнал при инцидент. Не описвайте отново техническите стъпки за настройване на Firewall.

Задача 3 Минимизиране на данните

Форма за записване в училищен клуб иска име, клас, контакт, ЕГН, домашен адрес и парола за електронната поща. Преценете кои полета са обосновани за целта и кои трябва да се премахнат. Напишете кратка информация за целта, достъпа и срока. Работете с измислени данни.

Задача 4 Компрометирана система

След инсталиране на непроверена програма от акаунта са изпратени непознати съобщения и част от файловете не се отварят. Опишете първите действия на потребителя, проверките на администратора и нарушените цели на сигурността. Разграничете признаците от доказаната причина.

Задача 5 Лични данни и сигнал

При публично споделяне списък с телефони посочете кои права и политики са засегнати. Намерете официалните указания на КЗЛД за жалба и за уведомяване при нарушение. Обяснете разликата между двете; не изпращайте реален сигнал за учебния казус.