Міжнародна тестова комісія

Керівництво Міжнародної тестової комісії з безпеки тестів, екзаменів та інших форм оцінювання

6 липня, 2014, Версія 1.0

Фінальна версія

Посилання на документ: ITC-G-TS20140706

Переклад:

Кірієнко Пелагея

Варто цитувати як:

INTERNATIONAL TEST COMMISSION (2014). ITC GUIDELINES on the SECURITY of TESTS, EXAMINATIONS, and OTHER ASSESSMENTS.

[HTTP://WWW.INTESTCOM.ORG]

Офіційно прийнято

Радою Міжнародної тестової комісії керівництво було офіційно прийнято під час зборів в Сан Себастьяні, Іспанія, в липні 2014 року.

Опубліковано онлайн

Цей документ був офіційно опублікований онлайн після Загальних Зборів МТК у липні 2014 року у Сан Себастьяні, Іспанія, і відтоді його можна знайти на веб-сайті МТК http://www.intestcom.org

Опубліковано в друкованому вигляді

Цей документ ще не публікувався в друкованому вигляді.

Будь ласка, посилатися на цей документ:

Міжнародна тестова комісія (2014). Керівництво МТК з безпеки тестів, екзаменів та інших форм оцінювання. [www.intestcom.org]

Подяка

Дані нормативи були підготовлені під керівництвом доктора Девіда Фостера з Kryterion, Inc. та Caveon Test Security (США), за підтримки Юджина Берка з SHL (Великобританія) і Кейсі Маркс, Cambridge Assessments (США). Під час роботи були використані різноманітні документи та публікації в сфері тестової безпеки, тому ми б хотіли подякувати всім помічникам в даній області, а також тим, хто приймав особисту участь в розробці нормативів, що містяться в цьому документі. Окрема подяка:

Девіду Бартраму (Великобританія)
Ієну Коєну (Великобританія)
Драгошу Ілієску (Румунія)
Тому Окленду (Сполучені Штати Америки)

Автор висловлює вдячність за докладені зусилля та цінні коментарі і пропозиції тих, хто допоміг на оглядовому етапі документа: Сарі Гутьєррес (з боку CEB SHL Talent Measurement), Вільяму Дж. Гаррісу (від Асоціації видавців тестів), Джону Хатті, Джону Кліману (з боку Questionmark), Фреді Лангу (від Консультативного комітету з діагностики та тестування Асоціації німецьких психологів), Пітеру Макквіну (з Групи контролю тестів та тестування Австралійської спільноти психологів), Маркусу Скотту (з боку Caveon Test Security) і Річарду Сміту (з Британської спільноти психологів).

Також ми хотіли б завдячити основним стандартам і керівництвам, що допомогли нам під час розробки тих матеріалів, які ви знайдете в цьому документі. Серед них:

- American National Standards Institute (ANSI) (2006). Guidance for Conformity to ANSI/ISO/IEC 17024: Requirement for Certification Program Security.
- American Educational Research Association (AERA), American Psychological Association (APA), & National Council on Measurement in Education (NCME) (1999). Standards for Educational and Psychological Testing.
- Caveon Test Security (2009). Test Security Standards.
- Association of Test Publishers (ATP) (2002). Guidelines for Computer-Based Testing.
- International Test Commission (ITC) (2005). International Guidelines on Computer-Based and Internet Delivered Testing.
- National Council on Measurement in Education (NCME) (2012). Testing and Data Integrity in the Administration of Statewide Student Assessment Programs.
- National Organization for Competency Assurance (NOCA) (2001). Certification Testing on the Internet.

На додачу, ми б хотіли висловити вдячність за вагомий внесок наступному текстовому джерелу, цілком присвяченому захисту тестів та оцінювання:

- Wollack, J. A. & Fremer, J. J. (2013). Handbook of Test Security. New York: Routledge.

Короткий огляд

За останні двадцять років істотно зросла кількість та серйозність загроз безпеці інформації і це дає підстави для сумнівів у валідності оцінювань, що проводяться в різних країнах. Загрози поширилися з багатьох причин, серед яких тенденція використовувати комп'ютеризовані чи онлайн-тести, а також застосування технологій, що вихоплюють і миттєво незаконно розповсюджують вміст тесту по всім куткам світу, і котрі майже неможливо виявити. Не існує оцінювальної програми, великої чи малої, цілком невразливої до цієї потенційної шкоди.

Міжнародна Тестова Комісія усвідомила критичну необхідність кожної організації, яка має важливу програму оцінювання, бути обізнаною щодо таких загроз та вміти протистояти їм. Саме для цього і розроблялись дані нормативи. Знаючи про загрози, є можливість вжити ефективних заходів для захисту програми та її ресурсів, тим самим зберігаючи цінність тестів і оцінювань для міжнародного суспільства.

Дане керівництво надає поради щодо планування захисту, дотримання заходів безпеки під час розробки та проведення тестів, а також правильного реагування на порушення безпеки. Дотримання цих інструкцій створить значний захисний бар'єр між зловмисниками і цінними ресурсами, розробка яких потребувала часу і грошей.

Зміст

Вступ

Цілі Керівництва МТК з безпеки тестів та інших форм оцінювання

Потреба в захисті тестів, екзаменів та інших форм оцінювання зросла з розвитком тестування та все більшим застосуванням технологій у поширенні, застосуванні та підрахунку результатів тестів, особливо за допомогою інтернету.

Усі зацікавлені в розвитку та використанні тестів погодяться, що цінність результатів тесту чи іншого структурованого оцінювання значно знижується у випадку шахрайства чи крадіжки тесту. Під шахрайством мається на увазі будь-яка спроба покращити результати тесту, екзамену чи оцінювання обманним шляхом. Крадіжка тесту – це спроба вкрасти вміст тесту до, під час чи після його запланованого проходження.

Головне призначення цих нормативів полягає в тому, щоб поділитися основними елементами досвіду, за допомогою якого розробники, спонсори, користувачі тестів, а також постачальники послуг тестування зможуть підтримувати безпеку своїх програм тестування та оцінювання, захистити цінність інформації, отриманої з результатів.

Шахрайство, крадіжка тестів та інші порушення можуть статися навіть із найсправнішою програмою. Проте, активна програма управління безпекою гарантує зменшення можливих порушень та шкоди, завданої ними.

Цільова аудиторія Керівництва

Багато зацікавлених осіб залучено у процес тестування та оцінювання. Порушення безпеки можуть торкнутися будь-кого, тому кожен може винести свою користь із знання та застосування даних нормативів. Нижче описані сім груп зацікавленої сторони:

- **Учасники тестів**. Люди, які особисто проходять тест чи оцінюються будь-яким іншим способом. Також вони можуть реєструватися, платити за тести та запланувати їх проходження на певний день.
- **Розробники тестів**. Особи чи організації, відповідальні за проектування та створення тесту чи оцінювання. Дані послуги можуть виконувати і сторонні працівники/організації.
- **Адміністрація постачальника послуг тестування**. Організації, які мають технології та канали поширення (наприклад, центри тестування) опублікованих тестів для їх доступності учасникам тестування в зручному місці та зручний час.
- **Служби безпеки тестування**. Дані служби пропонують спеціальні послуги безпеки (наприклад, судова експертиза) для підвищення рівня захисту. Служба безпеки тестування може бути частиною більшої службової організації, а може працювати незалежно.
- **Технологічні служби**. Організації, які надають різноманітні послуги зацікавленим сторонам проекту, включаючи послуги баз даних, інформаційного сховища, комунікаційні послуги, адаптаційні послуги, забезпечення збереження інформації тощо.
- **Власники або Видавці тестів**. Організації або особи, які мають права на контент тесту і дають дозвіл на його використання для конкретних цілей. Також, у разі необхідності, вони укладають контракт із поставниками різних послуг.
- **Користувачі тестів**. Користувачі тестів – зацікавлена сторона, що використовує тестові дані, зокрема результати, для прийняття індивідуальних чи колективних рішень, або ж для розробки тактики.

Як побудовано Керівництво безпеки

Ці нормативи стосуються ключових моментів, які забезпечують ефективний захист тестування та оцінювання. Серед них:

- **Розробка та виконання плану безпеки**, що в загальних рисах окреслює необхідну підготовку, включаючи створення плану реагування на інциденти, пов'язані з порушенням інформаційної безпеки, та встановлює заходи і методи для управління системою безпеки;
- **Впровадження захисту процесу тестування та оцінювання**, що охоплює як проектування та розробку тесту/оцінювання, так і адміністративні процедури використання тестів;
- **Реагування на порушення безпеки**, у разі виникнення ситуації шахрайства чи крадіжки тесту.

Як використовувати Керівництво на практиці

Ці нормативи призначені для міжнародного застосування. Велика кількість контекстних умов може вплинути на їх реалізацію на практиці. При виконанні нормативів потрібно розглядати ці умови на місцевому рівні. До них входять:

- Соціальні, політичні, інституціональні, лінгвістичні та культурні відмінності між умовами оцінювання;
- Закони, статути, принципи, інтернаціональні стандарти та інші юридичні документи, що регулюють проблеми тестування;
- Закони, прийняті в різних країнах, щодо регуляції проходження, зберігання та використання тестових даних;
- Існуючі національні нормативи та експлуатаційні стандарти, встановлені професійними спільнотами та асоціаціями.

Керівництво

Сфера використання нормативів

Масштаби тестового шахрайства підвищуються у разі тестування з високими ставками, коли результати тесту, екзамену чи структурованого оцінювання мають велике значення для учаснику тесту[1] і/або для інших зацікавлених сторін. Наприклад, коли йдеться про навчальні тести для отримання допуску до певної освітньої програми, отримання кваліфікації під час чи після завершення програми. В медичній сфері такі сценарії можуть включати рішення щодо клінічного лікування або юридичних процедур, які залежать від діагнозу, встановленого учаснику тесту. В умовах працевлаштування це стосується отримання посади чи підвищення співробітника компанії. Близькими до умов працевлаштування є ті, що мають відношення до оцінювання вмінь та навичок, завдяки яким учасники тесту отримують сертифікати та ліцензії, які підтверджують необхідний рівень їх професійної кваліфікації. У судовій сфері такі сценарії виникають під час проведення судово-психіатричної експертизи і вирішення щодо суворості покарання, якщо людину визнали винною.

Хоча ці нормативи сфокусовані на використанні тестів, враховуючи високий науково-практичний рівень проблеми безпеки тестування, приклади, наведені в попередньому абзаці, демонструють, що проблема безпеки має місце в будь-якому структурованому оцінюванні, яке використовується для оцінки знань, навичок, здібностей та психологічних особливостей людини. Наприклад, при працевлаштуванні, учасник тесту буде оцінюватися за допомогою інтерв'ю, до якого він може підготуватися, отримавши всі типові для такого інтерв'ю питання під час консультування. Спостереження за поведінкою на робочому місці чи в класній кімнаті становить ще одну форму оцінювання, на яке може вплинути порушення безпеки, особливо якщо спостерігач якимось чином зацікавлений у результатах спостереження. Хоча терміни *тест* і *екзамен* вживаються найчастіше, серед цих нормативів читач знайде інформацію, яка допоможе покращити рівень безпеки для всіх можливих типів оцінювання.

Значення оцінювання, що з самого початку планувалося як оцінювання з низькими ставками (наприклад, оцінка за методом 360 градусів потреб персоналу у навчанні та розвитку), може зрости в очах учасників тесту у разі усвідомлення важливості наслідків (наприклад, доступ до навчальних програм і програм розвитку забезпечить набуття якостей, які дають можливість отримати підвищення чи збільшення зарплатні). Зацікавлені сторони, ймовірно, знайдуть представлені в цьому Керівництві правила цінними, незалежно від вагомості оцінювання. Не дивлячись на універсальну користь цих нормативів, вони, усе ж таки, не поширюються на випадки, які не потребують тестової безпеки – наприклад, під час самооцінки чи пробних тестів.

Керівництво доволі часто рекомендує задіяти технології для запобігання та виявлення тестового шахрайства. Хоча тестування все частіше проводиться на комп'ютерах та в інтернеті, безпека тестування є актуальною для будь-якої форми проведення тесту чи оцінювання. І тому описані в даних нормативах правила поширюються в рівній мірі як на паперову форму чи мануальне тестування, так і на методи оцінювання із залученням технічних засобів і гібридні варіанти, де використовується більше одного способу проведення тесту.

Іншими словами, ціль даного Керівництва – сприяти захисту всіх типів тестування та оцінювання, незалежно від того, в сценаріях з якими ставками вони розгортаються – високими чи низькими, та впроваджувати найкращі інструкції використання як електронних, так і

[1] Учасник тесту і екзаменований – взаємозамінні терміни, які використовують, говорячи про осіб, що проходять тест, екзаменування, або оцінювання, як з високими, так і низькими ставками. В цих нормативах ми використовуємо «учасник тесту» і «екзаменований» для позначення осіб, які проходять тест чи оцінювання безвідносно до їх цілей і ставок.

мануальних тестів, визнаючи те, що представлені методи та рівні захисту можуть різнитися в залежності від типу і/або умов оцінювання.

Безпека – це не «все або нічого». Треба провести баланс між ризиком шахрайства та крадіжки з одного боку, і ціною їх профілактики – з іншого. Цей баланс залежить від ставок тесту. Дані нормативи прикликані охопити можливі дії для забезпечення максимальної безпеки, але слід зазначити, що не всі ці правил повинні безумовно дотримуватись в кожній ситуації. Підкреслюється необхідність аналізу ризику в кожному окремому випадку та здійснення таких заходів безпеки, що подолають або знизять цей ризик. Також важливо ретельно ознайомитись із планом безпеки всього процесу оцінювання.

Керівництво поділено на три частини: (1) Розробка та виконання плану безпеки, (2) Впровадження захисту процесу тестування та оцінювання, і (3) Реагування на порушення безпеки. Кожна з частин представлена нижче в зазначеному порядку.

Частина перша: Розробка та виконання плану безпеки

Основна термінологія для успішного забезпечення безпеки включає поняття загрози, ризику, вразливості та порушення. Підготовка успішної програми вимагає знання про існування певних загроз безпеці і про пов'язаний з ними ризик. Наприклад, вразливість та слабкі місця програми, а також недостатня підготовка персоналу підвищують рівень ризику. Розрахувати ризик можна неофіційно, з огляду на обставини в певний момент часу, наприклад:

- вірогідність того, що загроза матиме успіх,
- наскільки легко скористатися вразливістю програми,
- об’єм шкоди, що може завдати вдала спроба порушення,
- готовність програми виявити/зупинити порушення та ліквідувати негативні наслідки.

Проілюструвати дані приклади може реальний приклад. Оскільки в США поширене тестування із високими ставками, можна нарахувати велику кількість випадків порушення безпеки, що розслідувались в різних штатах, коли деякі шкільні адміністратори та вчителі були звинувачені в маніпуляціях із результатами тесту (порушення), а саме - в підміні бланків з відповідями, консультуванні та наданні студентам доступу до тесту до його проведення, а також в інших шахрайських методах, про які можна прочитати далі. Вірогідність виникнення спроби шахрайства, яке може завдати очікуваної шкоди (ризик), може бути завчасно проаналізована, якщо подивитись наскільки розповсюджені порушення в інших штатах, якої шкоди вони завдали, і прийняти до уваги відповідальність вчителів та адміністраторів за проведення тесту (вразливість). Порушення виникає тоді, коли трапляється і виявляється спроба шахрайства.

Аналізуючи ризик та продумуючи свої організаційні задачі, програма може приділити першочергову увагу тому, як використати свої обмежені ресурси для зменшення загрози, послаблення вразливості та задіяння механізмів виявлення та запобігання порушень.

Створення ефективного плану безпеки вимагає розуміння характеру поточних загроз безпеці програми та можливого ризику. Загроза безпеці є джерелом потенційного шахрайства та крадіжки тесту. Наприклад, існує загроза шахрайства в тому випадку, коли є можливість отримувати текстові повідомлення на мобільний телефон під час тестування. Загроза крадіжки тесту виникає в тому випадку, коли хтось отримує доступ до пристрою чи іншого місця зберігання інформації про тест, і заволодіває всім чи частковим вмістом тесту. З кращим усвідомленням певних загроз та ризиків для програми тестування, збільшується потреба в створенні та модифікуванні ефективного плану безпеки. Правильно розроблений та виконаний план безпеки знизить кількість загроз та пом’якшить завдану порушеннями шкоду.

В **таблиці №1** і **таблиці №2** перераховані можливі загрози шахрайства та крадіжки тесту (Foster & Miller, 2012).

Таблиця №1. ***Види шахрайства***

Вид	**Опис**
Попереднє ознайомлення з контентом тесту	Учасник тестування отримує дійсні питання з надійного джерела до проходження тестування.
Отримання кваліфікованої допомоги під час проходження тесту	Учаснику тесту допомагає вчитель або інший спільник.
Використання заборонених допоміжних засобів	Учасник тесту використовує недозволені допоміжні засоби під час тестування (наприклад, шпаргалки, мобільні телефони, навушники, програмовані калькулятори тощо).
Використання послуг підставної особи	Учасник тесту користується професійними послугами підставного тестування або ж за нього здає тест друг чи колега.
Підробка бланку відповідей чи результатів тесту	Після завершення тестування, особа (наприклад, вчитель) може підробити бланки відповідей, виправляючи неправильні відповіді на вірні. Як альтернатива – втручання в базу результатів тесту з метою підвищення балів.
Списування в іншого учасника тесту	Учасник тесту списує відповіді, дані іншим учасником під час тестування.

Таблиця №2. ***Види крадіжки тесту***

Вид	**Опис**
Крадіжка тестових файлів чи буклетів	Тестовий контент найбільш вразливий на певних етапах розповсюдження (наприклад, коли файли зберігаються на сервері чи тестові буклети – в камері зберігання). Неадекватний контроль режиму доступу дозволяє крадіям захопити контент тесту повністю, включаючи відповіді.
Крадіжка тестових питань за допомогою цифрових пристроїв з функцією фотографування чи копіювання	Питання тесту можуть бути вкрадені прямо під час тестування. Крадій може використовувати приховану чи таку, що важко виявити, високоякісну цифрову камеру або інший копіювальний пристрій (наприклад, ручки-сканери).
Крадіжка питань через запис вмісту тесту в електронному вигляді	Можлива в технологічних тестах, де увесь сеанс тестування, включаючи питання, може бути вкраденим за допомогою автоматизованої процедури через використання системи цифрового запису, підключеної до одного з портів виводу комп’ютера.

Вивчення контенту тесту	Учасник тесту запам’ятовує питання, щоб потім згадати та записати їх. Як частина організованого зусилля, такий вид крадіжки називається "збирання" ("harvesting").
Голосовий запис питань чи транскрибування	Усний чи письмовий контент може бути вкраденим під час тестування за рахунок використання пристроїв аудіо-запису чи запису тексту (наприклад, мобільні телефони, двосторонній радіозв’язок, блокноти та чернетки).
Придбання тестового матеріалу від "своєї людини"	Працівник або підрядчик тестової програми може викрасти вміст тесту під час його розробки, публікації чи розповсюдження.

Аналіз ризику допомагає вирахувати вірогідність загроз, описаних в Таблиці №1 та №2, разом із шкодою, яку вони можуть завдати, якщо спроба порушення буде вдалою. Далі два приклади.

Шахрайство зі сторони принаймні однієї особи – ймовірне, і навіть є звичайною ситуацією для будь-якої програми тестування. Шкода від нього зазвичай обмежується одиничним неточним рішенням, прийнятим на основі одиничного неправильного тестового результату. Однак викрадений та розповсюджений онлайн-тестовий буклет, може спричинити значне покращення тисячі чи десятків тисяч чиїхось результатів. Вірогідність такої ситуації мала, однак вона може завдати великої шкоди. Організація має встановити: скільки ресурсу для виявлення та протидії окремим шахраям вона може виділити, або які процедури запровадити з метою профілактики крадіжки та розповсюдження тестових буклетів.

Таблиці №1 та №2 демонструють систематику декількох видів загроз відомих сьогодні. Однак для кожної категорії існують сотні реальних *методів* шахрайства чи крадіжки тесту. Наслідуючи приклад банківської галузі, повномасштабна безпека повинна забезпечуватися багаторівневими захисними процедурами, враховуючи те, що декілька одночасно задіяних методів будуть більш ефективними, ніж застосування одного методу. Ці рекомендації призначені для сумісного використання для підготовки ефективної програми дослідження ризиків безпеки.

Вказівки щодо розробки та виконання Плану безпеки

Документ з викладом Плану безпеки необхідний для підтримки цілісності та недоторканості всіх тестових і оцінювальних матеріалів, а також результатів тесту і рішень, прийнятих на їх основі.

1. Документ повинен визначити ролі та обов’язки щодо забезпечення безпеки на всіх етапах процесу – планування та розробка, впровадження, збір/збереження/аналіз результатів, розповсюдження та проведення. Може включати всі чи деякі з наступних ролей:
    a. **Директор з питань безпеки**. Коли є така можливість, програма повинна передбачати Директора з питань безпеки, який відповідає за всі аспекти забезпечення безпеки.
    b. **Комітет з питань безпеки**. Програма повинна передбачати Комітет з питань безпеки (очолений Директором з питань безпеки), який складається з осіб, відповідальних за створення та підтримку плану безпеки, оцінку тяжкості інцидентів та вжиття заходів у випадку їх виникнення, здійснення контролю за реакціями на порушення безпеки, іншими діями, що забезпечують реалізацію плану безпеки.

c. **Менеджери**. Особи, що несуть відповідальність за розробку тесту, проведення тесту, збір і збереження результатів, повинні проходити відповідну підготовку щодо виконання заходів і процедур, передбачених планом безпеки.
d. **Інспектор, Спостерігач чи Адміністратор тестування**. Люди, що відповідають за безпечне проведення тесту, включаючи аутентифікацію та ретельний моніторинг учасників тесту під час тестування. Інспектори і/чи Адміністратори не повинні надавати послуг інструкторів, профільних експертів, тренерів і будь-кого іншого, хто має доступ до інформації, що оцінюється за допомогою тесту, оскільки це може спровокувати конфлікт інтересів і вплинути на результати оцінювання.
e. **Постачальники послуг безпеки тестування**. Особи, що сприяють виявленню вразливості, слабких місць програми, допомагають передбачити можливі проблеми безпеки, виявляють порушення, коли ті виникають, оцінюють масштаби шкоди, рекомендують заходи і, можливо, вживають ці заходи. До цих професіоналів входять консультанти, дослідники, аналітики комп'ютерної криміналістики, спеціалісти по веб-контролю, правові експерти тощо.

2. Документ Плану безпеки повинен детально описувати права та обов'язки учасників тесту під час тестування чи оцінювання та спосіб підтвердження учасником своєї обізнаності щодо цих прав та обов'язків.
   a. Учасник тесту має право проходити безпечне оцінювання з високими ставками, так, щоб жодний учасник не мав несправедливої переваги за рахунок списування чи інших форм тестового шахрайства.
   b. Учасники тесту, запідозрені чи звинувачені в шахрайстві, мають право на правові гарантії.
   c. Учасники тесту несуть відповідальність за нерозголошення контенту тесту та зобов'язанні повідомити про випадки такої діяльності.
3. Документ Плану безпеки повинен бути доступним для всіх зацікавлених сторін.
4. План безпеки повинен включати план заходів у випадку порушення із зазначенням дій у разі виникнення ситуації порушення безпеки. План заходів повинен включати цілі, графіки, основний склад фахівців, систему звітності, положення про розголошення інформації, контакти із ЗМІ та певні варіанти коригувального впливу, відповідно до характеру інциденту чи порушення. Окрім того, коригувальний вплив має включати санкції для порушників, анулювання або визнання результатів недійсними, процедуру повторного тестування, заміну тестових форм і судовий процес.
5. План безпеки повинен чітко зазначити правила безпеки, які, в свою чергу, потрібно донести до всіх зацікавлених сторін. Наслідки порушень цих правил повинні бути зрозумілими.
6. План безпеки повинен бути схвалений відповідною групою зацікавлених сторін і переглядатися хоча б раз на рік.
7. План безпеки повинен документувати вимоги щодо безпеки процедур і стратегій інформаційно-комунікаційних технологій (ІКТ) для працівників, підрядчиків та всіх постачальників послуг. Ці вимоги розглядають безпечне збереження та доступ до тестового контенту, результатів, даних учасника та захист інформації під час зв'язку і передачі.
8. План безпеки повинен містити відсилки до прав власності різних країн та регіонів, в яких може проводитися тестування. План повинен зазначити, як змінюються стратегії і процедури для пристосування до цих відмінностей. Захист даних окремих осіб чи організацій має бути узгоджений із дійсними законами та правилами.
9. Необхідна наявність достатніх коштів для здійснення профілактики та моніторингу передбачених в документі заходів. Крім того, повинен існувати резервний фонд на випадок виникнення можливих серйозних порушень. Слід регулярно переглядати бюджет – він повинен відповідати потенційним загрозам.

10. Повинні бути створені навчальні матеріали з питань безпеки, пов'язані з ролями та обов'язками, зазначеними в документі Плану безпеки. Всі особи, залучені до тестового підприємства, мають ознайомитись із цими матеріалами.
11. Нерозголошення та інші домовленості повинні укладатися в плановому порядку усіма сторонами, включаючи учасників тесту, постачальників послуг та працівників програми. Ці домовленості вимагають визнання авторського права та права власності на контент тесту чи оцінювання, ознайомлення з тим, яка діяльність вважається шахрайством, і які наслідки вона може понести за собою. Дані угоди вимагають підтвердження осіб, що вони не будуть розголошувати запатентовану інформацію.
12. Власник тесту повинен придбати авторське право чи іншим законним шляхом встановити право власності, щоб захистити контент тесту в країнах, де буде проводитися тестування.
13. Процедури безпеки всіх постачальників послуг мають час від часу проходити контроль та облік для оцінки ефективності. Це можуть здійснювати експерти з внутрішньої та зовнішньої безпеки.

Частина друга: Впровадження захисту процесу тестування та оцінювання

Після розробки схваленого Плану безпеки, можна продумувати, створювати, здійснювати та проводити заходи безпеки процесів, що виникають до/під час/після тесту або оцінювання. Важливі етапи процесу тестування чи оцінки, що можуть мати наслідки для безпеки, включають:

- Реєстрацію учасника тесту
- Ідентифікацію особистості учасника тесту
- Моделювання тесту та його елементів
- Розробку тесту
- Публікацію та розповсюдження тесту
- Проведення тестування
- Підрахунок та аналіз результатів тесту
- Збір та тривале зберігання результатів тесту, інформації про учасників

Більша частина даних процесів вимагає поширення матеріалів серед зацікавлених сторін.

Вказівки щодо Впровадження захисту процесу тестування та оцінювання

1. Учасники тесту повинні бути зобов'язані проходити формальну реєстрацію для оцінювання. Реєстрація для планування та проведення тесту чи оцінювання повинна включати, як мінімум, надання унікального імені користувача та логіну або паролю кожному учаснику тесту.
2. При реєстрації або плануванні дати проходження, необхідно інформувати учасників про належні процедури аутентифікації. Організатори можуть знати учасників тесту або видавати їм організаційне посвідчення особи. В іншому випадку, учасників тесту можуть попросити надати верифіковану інформацію, наприклад, легальні документи державного зразка з фотографіями, або прийняти участь в процедурах біометричної ідентифікації. В деяких тестових процедурах необхідно інформувати учасників про необхідність ідентифікації після сеансу тестування (наприклад, при використанні скринінг-тестів під час оцінювання при влаштуванні на роботу).
3. Реєстраційні процедури забезпечують доступ лише відповідних зареєстрованих осіб до тестування чи оцінювання. Вимоги для доступу можуть включати проходження навчання, здачу попереднього тесту або внесення платежу. В деяких випадках необхідно зазначити, скільки часу має пройти перед тим, як можна буде знову пройти тестування.

   a. Якщо це дозволено і не суперечить законам про недоторканність, можливе створення списку «обмежених» учасників тесту, які з високою вірогідністю здатні на порушення. Звіряючись з цим списком, онлайнові та оффлайнові системи реєстрування/планування можуть забороняти або обмежувати тестування для цих індивідів за встановленими програмою правилами.
4. Повинні бути розроблені стандарти повторного тестування, щоб скоротити можливість крадіжки тестового контенту та інших форм шахрайства. Наприклад, учасник тесту не зможе перескласти тест, який він уже «здав», або поки не пройде встановлений період часу.
5. Щоб учасники тесту не складали тест частіше, ніж це дозволено, реєстрація повинна проходити під пильним наглядом. Це зменшить вірогідність шахрайства.
6. Слід розробляти тести з обмеженням показу питань чи зі зміною їх порядку, зберігаючи психометричні властивості. Під час такої розробки необхідно вирішити як будуть підбиратися та подаватися питання і завдання тесту (наприклад, у вигляді комп'ютеризованого адаптивного тесту, лінійного адаптивного, багатоступінчастого чи тесту із множинним вибором), чи буде надана можливість повертатися до певних завдань по ходу тесту, чи буде задіяне правило завчасної зупинки.
   a. В деяких видах тестів, коли надано достатньо відповідей для отримання результату чи прийняття рішення з належним рівнем надійності, програма може завершити появу нових питань чи завдань, таким чином уникаючи непотрібного демонстрування решти контенту.
   b. Показ питань також може бути розробленим таким чином, що закінчиться або зміниться в тому випадку, якщо учасник тесту незацікавлений або намагається шахраювати, викрасти питання, хворіє, почувається ослабленим або ще з якихось причин не може або не хоче сприяти адекватному оцінюванню.
7. Програми повинні розглядати варіант із односпрямованим показом питань, що не дозволить учасникам тесту збирати або накопичувати питання для потенційної крадіжки (наприклад, через запам'ятовування або цифрову зйомку). Деякі види тестів або питань є більш захищеними, якщо в них обмежена чи відсутня можливість помічати та повертатися до певних питань (як в комп'ютеризованих адаптивних тестах).
8. Демонстрація контенту тесту або оцінювання повинна активно контролюватися. Наприклад, розробникам слід створювати такі оцінювання, де можливість вибору питання із резерву не переходить в незаплановане і неконтрольоване розповсюдження питань.
9. Більші резерви питань спряють процедурам контролю та управління використання і розповсюдження питань/завдань тесту.
10. Завдання повинні бути зроблені із контролем та обмеженням показу контенту. Існує багато способів це зробити. Варто звернути увагу на можливу потребу змінити існуючі системи розробки тестів, платформи для експлуатації програм та системи зберігання бази даних, щоб пристосувати нові типи та альтернативні формати (наприклад, формат вимушеного вибору в опитувальниках самооцінки, симуляція, використання мультимедійних засобів, інтерактивні тести з перетягуванням мишею).
   a. При використанні форматів з множинним вибором, можна не показувати всі можливі відповіді на питання (наприклад, варіанти показуються один за одним доки не буде надана вірна чи невірна відповідь, або учасник буде витягувати потрібні варіанти відповідей з більшого набору – і це лише окремі варіанти тесту із множинним вибором).
   b. У форматах із множинним вибором, варіанти відповідей можуть подаватися у довільному порядку, плутаючи учасників тесту, які мали можливість ознайомитись з контентом тесту наперед.
   c. Використання відео, аудіо, симуляцій та інших медійних форм може ускладнити захват тестового контенту і попередити шахрайські дій.

11. Щоб підтвердити результати тестування в менш безпечних умовах, можна вимагати підтвердження або верифікації. Процес верифікації має здійснюватися за згодою учасника тесту.
12. Спираючись на статистику, слід встановити точні часові обмеження, які б надавали можливість спокійно завершити тест, і в той же час зменшити можливість шахрайських дій чи крадіжки вмісту тесту.
13. Контент тесту повинен бути ретельно захищеним на стадії розробки, адже питання і тести проходять чимало етапів роботи, де психометристи, редактори, профільні експерти та інші фахівці мають до них вільний доступ.
    a. Тести та завдання тестів мають бути захищені шляхом обмеження їх розповсюдження, доступ до них повинні мати лише ті, хто приймає участь в їх розробці та рецензуванні і лише на обмежений період часу.
    b. Повинні бути задіяні суворі процедури контролю доступу такі, як використання логінів та паролів або біометрична аутентифікація.
    c. Ті, хто мають доступ до тестів та їх вмісту, мають проходити спеціальну перевірку даних і укладати договір про нерозголошення інформації.
    d. Тести та завдання, направлені до інших серверів для рецензування, тимчасово виходять з-під безпосереднього контролю, тому повинні бути негайно знищені одразу після рецензування та внесення змін. Факт видалення повинен бути підтвердженим.
    e. Право на власність тестових завдань (наприклад, авторське право) має бути встановлено відповідно до державних правил і стандартів.
    f. Особи, залучені до процесу розробки, повинні вміти розпізнавати та повідомляти про порушення безпеки.
14. Тест повинен бути захищеним під час розробки, публікації та розповсюдження.
    a. Сервери, на яких зберігається тестовий контент, повинні розміщуватися на професійних центрах обробки і передачі даних, сертифікованих за міжнародними стандартами (напр., ISO 27001 або SSAE 16). Також вони повинні використовувати заходи безпеки ІКТ (наприклад, брандмауери і програми для виявлення вторгнень).
    b. Особи, що працюють над тестами, мають бути надійними. Також вони зобов’язані укласти угоду про нерозголошення.
    c. Коли контент тесту випускається у вигляді буклетів чи цифрових файлів, він повинен бути захищеним на кожному етапі процесу розповсюдження і зберігатися в надійному місці. Служби надання послуг комп’ютерного або онлайн-тестування повинні відстежувати оновлення та одразу встановлювати патчі, які забезпечують усунення помилок захисту, для авторизованої операційної системи і програмного забезпечення.
    d. Цифровий контент повинен захищатися надійною схемою шифрування, незалежно від того, чи він повністю надсилається на віддалений сервер, звідки може бути завантаженим, чи кожне завдання відсилається одне за одним в режимі реального часу під час Інтернет-тестування.
    e. Тестовий контент, що знаходиться на сервері центру тестування будь-який проміжок часу, завжди повинен бути захищеним контролем доступу користувачів (наприклад, логіном та паролем) та надійними схемами шифрування.
    f. Тести повинні залишатися у місцях проведення тесту на мінімальний, визначений стандартами програми та адміністрації тесту, проміжок часу.
    g. Якщо тест більше не потрібен на місці проведення тестування, контент треба видалити і/або знищити. Видалення чи знищення повинні бути підтверджені, а контент не повинен відновлюватися.
    h. Розробники повинні упевнитися, що весь важливий матеріал чітко задокументований і може відстежуватись, зокрема, його повернення і/або

знищення, чи розміщення (якщо це дозволено) після використання. Повернення або знищення матеріалу повинно бути підтверджено.

15. Методи відстеження (наприклад, паперові чи цифрові протоколи) повинні використовуватися для запису етапів контролю, доступу та змін, внесених до файлів.
16. Учасники тесту повинні знати правила безпеки та усвідомлювати наслідки у разі їх порушення до реєстрації та планування тестування.
    a. Слід завчасно повідомити учасників тесту (наприклад, за допомогою кодексу честі чи етичних засад тестування), зобов'язавши їх прочитати, ознайомитись та погодитися із дотриманням правил безпеки до початку тесту.
    b. Наслідки порушення правил безпеки повинні бути зрозумілими.
    c. Учасники тесту повинні мати можливість як погодитися, так і не погодитись з цими правилами до початку тестування. У разі непогодження, учасникам заборонено проходити тест.
    d. Документація відносно прав учасника тесту повинна бути представлена та пояснена.
17. Учасники тесту повинні бути аутентифіковані[2] належним чином, якщо передбачено чинним законодавством. Це може відбуватися до, під час чи після тесту. До прийнятних методів аутентифікації входять: пред'явлення посвідчення особи з фотографією, використання біометричних засобів, як, наприклад, дактилоскопічний зчитувач, сканер долонь, іридосканер, клавіатурний почерк або розпізнавання рис обличчя.
18. Тести знаходяться у найбільшій небезпеці під час проведення тестування та після аутентифікації. Наприклад, в цей період представлені завдання можуть бути вкрадені; можливі інші форми шахрайства. На додачу до попередньо узгоджених заходів під час етапів планування та розробки, треба докласти додаткових зусиль, щоб застрахуватись від крадіжки тестового контенту і впевнитись, що ризик шахрайства значно знижений.[3]
    a. Система тестування повинна використовувати програму блокування або захищений браузер для обмеження операційної системи і робочої станції тестування так, щоб доступ до зовнішніх ресурсів обмежувався необхідними для завершення тесту.
    b. Інспектори повинні мати можливість запускати тест, використовуючи спеціальний «ключ», наданий системою тестування. Схожий ключ може надаватися учаснику тесту так, що для запуску тесту будуть необхідні обидва ключі.
    c. Інспектори зобов'язані пильно слідкувати за учасниками тесту, не заважаючи їм. Якщо це дозволено чинним законодавством, інспекція може проходити дистанційно, онлайн (через веб-камери) чи локально (на місці, з відеоспостереженням).
    d. Інспектори майже або взагалі не повинні мати можливості дивитися на монітор або сторінки буклету тесту учасника під час тестування.
    e. Інспектори повинні бути обізнані про очікувані методи як шахрайства, так і крадіжки тесту, та добре навчені щодо дій у випадках порушення безпеки, включаючи складення акту про порушення умов проведення тестування.
    f. Інспектори повинні бути достатньо вмотивовані для відстеження проблем безпеки та викриття учасників тесту, що підозрюються у порушенні.
    g. Інспектори не повинні бути зацікавленими в результатах тестування. Вони не мають бути інструкторами чи вчителями учасників тесту, а також знайомими із контентом тесту.

---

[2] Аутентифікація – не те ж саме, що й ідентифікація. Для екзаменів чи оцінювання з високими ставками неважливо встановлювати саме особистість людини. Необхідно лише впевнитись, що здаватиме тест та сама особа, що реєструвалася та підписувалася для програми.

[3] Те, що може виникнути, або виникне спроба шахрайства – це аксіома, навіть якщо було вжито найефективніших заходів безпеки. Ціллю програми забезпечення безпеки є обмеження шкідливого впливу від крадіжки тесту та зменшення загроз шахрайства до прийнятного рівня.

h. Якщо це дозволено чинним законодавством, на місці проведення повинні бути камери для допомоги у спостереженні, запису і збереження процесу тестування, можливих інцидентів безпеки.
i. Якщо це можливо і дозволено чинним законодавством, засоби, що можуть допомогти в потенційному шахрайстві чи крадіжці тестового контенту (наприклад, смартфони, записні книжки, камери, шпаргалки) необхідно зібрати до початку тестування та повернути по його завершенні.
j. Дозвіл на перерви має здійснюватися з великою обачністю. Після перерви учасники тесту не повинні мати можливості повернутися до питань, які вони пройшли до перерви.
k. Роздані та використані під час тестування бланки необхідно зібрати після тестування та обійтися з ними встановленим правилами безпеки чином.
l. Якщо під час тесту виявлено шахрайство чи спроба крадіжки вмісту тесту, необхідно діяти швидко та ефективно, згідно з наданою інструкцією. Це може потребувати тимчасової зупинки або припинення сеансу тестування, конфіскації приладдя або матеріалів, укладання офіційного акту про порушення безпеки.

19. У разі отримання цифрових результатів тесту з віддалених серверів, передача даних повинна здійснюватися відразу після завершення тесту чи після завершення кожного завдання під час онлайн-тестування. Дані повинні бути захищені надійними процедурами доступу та криптостійким шифруванням при їх передачі.
20. Тести та тестові завдання повинні регулярно оцінюватися на предмет шахрайства чи компрометації. Проведення тесту зміниться, якщо питання були вкрадені та розповсюджені, і якщо стався випадок шахрайства. Ось деякі приклади:
    a. Нетипові схеми відповідей (наприклад, коли на прості питання дають неправильні відповіді, у той час як відповіді на складні питання – вірні) можуть вказувати на шахрайство чи крадіжку.
    b. Незвична кількість часу витрачена на відповідь (наприклад, відповідь на питання зайняла надто мало або багато часу) може вказувати на порушення безпеки або іншу проблему.
    c. Багато виправлень на паперовій формі відповідей, зокрема виправлення із неправильних відповідей на правильні, можуть вказувати на отримання кваліфікованої допомоги під час тестування або підробку бланку відповідей (наприклад, вчителем).
    d. Надзвичайна схожість відповідей серед пар або груп учасників може вказувати на узгоджені дії або на поведінку підставного учаснику тесту.
    e. Схожі відповіді та приховані схеми декількох учасників можуть вказувати на узгоджені дії, тестування підставної особи або консультативну допомогу.
    f. Незвичайно високий результат групи або одного учасника тесту, що повторюється від одного сеансу тестування до іншого, може вказувати на шахрайство.
    g. Незвичайні зміни в статистиці виконання певних завдань можуть вказувати на їх скомпрометованість. Скомпрометовані завдання повинні бути негайно замінені.
    h. Різниця у виконанні завдань одного класу у порівнянні з іншими можуть вказувати на попереднє ознайомлення з контентом тесту. Наприклад, відповіді на завдання типу «троянський кінь» (де завдання змінено таким чином, що від початку правильна відповідь виявляється невірною), чи відповіді на включені в тест неоцінювані питань у порівнянні з відповідями на оцінювані, можуть вказувати на попереднє ознайомлення із контентом.
    i. Якщо це дозволено чинним законодавством, задля виявлення можливої спроби шахрайства можна проаналізувати демографічні дані учасників тесту (наприклад, поведінку підставного учасника). Те, що учасник, який проживає в одній країні, але не один раз складав тести в інших країнах за короткий проміжок часу, може

вказувати на спробу підставного тестування або узгодження дій зі сторонньою особою.

j. У разі регулярного графіку тестування, можна відстежувати тривалість часу, витраченого на проходження тесту. Якщо проходження тесту виходить за рамки звичайної тривалості, це може вказувати на спробу шахрайства або крадіжки контенту.

21. Програмне забезпечення для авторської розробки іспиту, його складання або адміністративних цілей програми, повинно бути розроблено із використанням процедур безпеки, що запобігають виникненню вразливості програмування та періодично оцінюються (наприклад, тестуванням сторонніх організацій на можливість проникнення).
22. Підрахунок результатів технологічних тестів у більшості випадків проводиться після завершення тесту або під час тестування після кожного питання, на яке була дана відповідь (наприклад, автоматизоване тестування). Для таких тестів загроза та ризик шахрайства мінімальні. Процес підрахунку балів для паперових тестів надто довгий та складається з декількох етапів, вимагаючи більших заходів безпеки для попередження зміни результатів.
    a. Бали і результати можуть бути доступними одразу, однак вони будуть підтвердженими лише після визначення їх валідності. Так, результати не можуть бути офіційно опубліковані, поки не будуть розглянуті всі повідомлення про порушення і не буде завершена криміналістична експертиза даних.
    b. Підрахунок та аналіз результатів комп'ютеризованого тесту повинен проходити з використанням надійно захищених віддалених серверів, а не комп'ютерів учасника тесту. Якщо говорити про паперові тести, існує ризик маніпуляцій із бланками відповідей після того, як їх зібрали та повернули до місць проведення сканування та підрахунку результатів. Повинен здійснюватися процес моніторингу для утримання паперових бланків під пильним наглядом і захистом до завершення їх використання для підрахунку балів.
23. Тести, їх питання та результати тестів, інша важлива інформація (наприклад, демографічні дані учасника) часто зберігаються протягом довгого періоду часу (іноді роками) – як паперові, так і цифрові. Незалежно від того, коли і де ця інформація була створена та зібрана, повинні бути встановлені професійні процедури для попередження небажаного доступ до цієї інформації (наприклад, злому), можливості перегляду результатів та інших даних, внесення змін та видалення без належної авторизації. Необхідно періодично перевіряти та оновлювати процедури та системи інформаційно-комунікативних технологій.
24. До, протягом чи після проведення тесту програма повинна почати процес моніторингу інтернету на предмет розголошення тестового контенту. Прикладом розголошення може бути бесіда деяких користувачів на тему тестування чи його окремого питання; або це може бути точне відтворення одного чи всіх тестових питань. У такому випадку програма повинна надіслати стандартний запит до адміністратора сайту для припинення обговорення та винесення попередження учасникам щодо видалення контенту. Можуть розглядатися суворі методи, в т.ч. судові позови, у випадку, якщо матеріали не були швидко видалені.
25. До, протягом або після часу проведення тесту, програма має захищати вміст тесту від розголошення стороннім особам, які не є авторизованими учасниками тесту або представниками програми тестування, які мають право на перегляд контенту.

Частина третя: Реагування на порушення безпеки

Загроза прорвалася крізь захист програми, що вилилося в успішну спробу шахрайства чи крадіжки контенту. Приведені нижче нормативи дають поради та підтримку для вирішення таких ситуацій. Якщо стався випадок шахрайства чи крадіжки тесту або його питань, програма тестування зобов'язана провести ретельне розслідування, зупинити порушення, відшкодувати збитки та вжити інших актуальних заходів. Також треба вжити профілактичних заходів, щоб попередити виникнення порушення в майбутньому.

Комітет безпеки повинен несе повну відповідальність за реагування на порушення безпеки і має вповноваження у прийнятті рішень.

Програма може дізнатися про всі можливі та дійсні порушення різними способами, деякі з них кращі та простіші за інші. Наприклад:

- З новин чи інших засобів інформації
- Зі звіту інспектора про порушення
- З приватно отриманих відомостей
- З судової експертизи даних
- Зі звітів про результати веб-моніторингу
- З автоматизованих "систем" безпеки (наприклад, недоречне натискання певних клавішних комбінацій; спроба вторгнення в систему)

Незалежно від джерела загрози, програма тестування повинна діяти швидко, щоб встановити достовірність та масштаби порушення. Під час тестування, система моніторингу чи інспектування повинна вживати невідкладних заходів при виявленні порушення. До і після тесту, комітет безпеки несе відповідальність за перегляд деталей порушення та відповідне реагування.

Вказівки щодо Реагування на порушення безпеки

1. Тестування учасника тесту повинно бути призупинено чи припинено, якщо адміністраторами тесту чи інспекторами (як онлайн, так і тими, що перебувають на місці тестування) була виявлена спроба шахрайства або крадіжки тесту. Причина повинна бути пояснена учаснику тесту.
    a. Після допиту запідозреного в шахрайстві чи недотриманні правил тестування учасника, інспектор чи адміністратор тесту може дати дозвіл на продовження сеансу тестування або вирішити, що він має бути призупинений або відмінений.
    b. Будь-які неприйнятні матеріали мають бути конфісковані, якщо це дозволено діючим законодавством. Учаснику тесту надають пояснення необхідності таких дій.
    c. Інспектор, наглядач або адміністратор тестування повинен скласти звіт про порушення та направити його до комітету безпеки програми тестування.
    d. Якщо тестування дозволено продовжити, комітет безпеки повинен підготувати та переглянути звіт про порушення під час тестування.
2. Порушення потребує ретельного розслідування для оцінки його поширеності та масштабу завданої шкоди. Розслідування може включати: інтерв'ю з особами, що можуть бути причетні, або зі свідками; судову експертизу даних для оцінки впливу на результати; веб-моніторинг для встановлення рівня розголошення тестового контенту.
3. Скомпрометований тест або питання тесту повинні бути якнайшвидше замінені.
    a. Деякі програми можуть використати раніше створений тест як аварійний варіант на випадок крадіжки тесту чи його завдань.
4. Результати, визнані недостовірними у зв'язку з шахрайством, повинні бути відмінені або визнані недійсними.

   a. Полегшити цей процес може наявність заходів перевірки в установленому порядку і визначення «тимчасових» підрахунків і тих, що очікують підтвердження.
   b. Якщо недійсні результати тесту вже були представлені учасникам тесту, необхідно негайно зв’язатися з ними та повідомити, що їх результати вважаються недійсними, а прийнятті на їх підґрунті рішення - будуть переглянуті.
5. Повторний аналіз результатів скомпрометованого тестування необхідний для забезпечення достовірності результатів для прийняття рішень (наприклад, після виявлення та усунення скомпрометованих завдань).
6. В залежності від прийнятих програмою правил та від масштабів завданої порушенням шкоди, можуть потребуватися додаткові дії, включаючи цивільний або кримінальний судовий процес.
7. Необхідно зв'язуватися з веб-сайтами, які пропонують продаж питання, захищених авторськими правами, без дозволу, з вимогою усунути весь контент з сайту та інших ресурсів. Веб-сайт необхідно ретельно контролювати, щоб впевнитися у видалені контенту.
   a. Офіційний представник програми може надіслати лист адміністратору сайту, вказуючи на проблему з вимогою видалення матеріалу. Такий підхід є ефективним, адже більшість адміністраторів швидко реагує і йде на зустріч.
   b. Якщо матеріали залишаються на сайті, можна надсилати офіційні письмові попередження про порушення прав інтелектуальної власності, погрожуючи порушенням кримінальної справи, якщо контент не буде видалено з сайту. При цьому можна посилатися на релевантні державні чи регіональні статути (наприклад, закон про авторське право в цифрову епоху).
8. В залежності від заходів та тяжкості порушення, учасникам може бути запропоновано та дозволено пройти той самий тест знову, у тому ж чи іншому вигляді. Якщо це дозволено діючим законодавством, причетним до шахрайства учасникам тесту може бути відмовлено у повторному тестуванні.
   a. Директивні документи повинні чітко вказувати правила повторного тестування, спільно узгоджені всіма зацікавленими сторонами, включаючи учасників тесту, перед проведенням тестувань.
   b. Для повторного тестування слід використовувати нову форму тесту, у разі її наявності.
   c. Додаткові умови (наприклад, грошовий внесок або відтермінування) можуть застосовуватися як умова повторного тестування.
9. Внаслідок порушення, може виникнути жвавий інтерес зацікавлених осіб та третіх сторін (наприклад, ЗМІ) і/або громадськості. У такому випадку необхідно розробити та розповсюдити документи ефективної комунікації. Можна скористатися послугами організацій зв’язків з громадськістю та/або прес-секретаря. Підготовлені матеріали можуть включати в себе стандартизовані повідомлення про виникнення порушення, його тяжкість та інформацію щодо вжитих заходів.
10. Після виникнення порушення, необхідно переглянути існуючий план безпеки та відповідні процедури для вирішення, чи потрібні зміни існуючих директив і процедур безпеки, включаючи додаток нових. Про зміни, якщо вони були внесені, необхідно повідомити всі зацікавлені сторони, після чого провести нову ревізію плану безпеки і ухвалити його.

Терміни та визначення

Аналіз ризику – аналіз різних загроз безпеці програми тесту з метою оцінки ризику, потенційних збитків, а також необхідних ресурсів їх для попередження.

Аутентифікація – процес визначення того, що людина які прийшла, проходить або готується пройти тест, це та сама людина, яка повинна його пройти. Аутентифікація відрізняється від ідентифікації, яка, у свою чергу, намагається встановити особистість людини.

Біометрія – метод збору унікальної інформації про людину з метою її ідентифікації чи аутентифікації.

Блокування клавіш – система блокування клавіш під час комп'ютерного та інтернет-тестування, яка обмежує можливість використання кнопок клавіатури лише необхідними для надання відповідей та навігації в програмі тестування. Доступ до інших ресурсів, жорсткого диску та інтернету заблокований до завершення тестування.

Вбудовані елементи – розміщення неоцінюваних пунктів для виявлення спроби шахрайства шляхом попереднього ознайомлення з правильними відповідями.

Веб-моніторинг – набір методів пошуку в інтернеті запитань тесту з поточного тестування.

Верифікаційний тест – тест, який дається досліджуваному через певний час з метою оцінки дійсності його попередніх результатів.

Визначення різниці продуктивності – метод судової експертизи даних, який здійснюється шляхом аналізу результатів, одержаних в різних умовах (наприклад, порівняння перших результатів із результатами через півроку), допомагає визначити, що тест був скомпрометований.

Випробуваний – особа, яка проходить тестування. Також згадується як Учасник тесту.

Вразливість – слабкі місця в захисті безпеки тесту.

Динаміка натискання клавіш – біометричний метод, під час якого відбувається порівняння між способом натискання клавіш учасником тесту під час реєстрації та безпосередньо перед початком тесту.

Допоміжні засоби – пристрої або документі, які можуть використовуватися під час тестування. Варто звернути увагу, що використання деяких пристроїв (наприклад, калькуляторів), може бути дозволеним.

Загроза – будь-яка особа або метод, який потенційно може призвести до успішного випадку шахрайства або захоплення тестового контенту.

Загроза пунктам тестування – виявлення негативного впливу на окремі пункти тесту, у зв'язку з чим вони більше не можуть використовуватися.

Збирання пунктів – спроба незаконного захоплення тестового контенту та обходження програмних правил безпеки.

Звіт про порушення - звіт, що надається інструктором або іншою особою, з приводу випадку шахрайства або іншого фактору, який мав вплив на процес тестування.

Змовники – особи, які працюють разом з метою шахрайства або викрадення контенту тесту.

Ідентифікація – процес встановлення особистості людини, що прийшла на тестування або готується скласти тест. Ідентифікація відрізняється від аутентифікації, яка не намагається встановити конкретну особистість.

Інспектор – людина, яка відповідає за безпеку тесту під час тестування. Також згадується як Спостерігач.

Крадіжка тесту – будь-яка поведінка спрямована на захоплення окремих пунктів або всього контенту тесту.

Латентний аналіз – метод судової експертизи даних, який вираховує час між появою питання та наданням відповіді учасником тесту. Надто довгі або надто короткі часові проміжки можуть свідчити про шахрайство або інше порушення безпеки.

Односпрямований показ питань – елементи тесту демонструються лише вперед, без можливості повернення до раніше переглянутих пунктів.

Оцінка зростання – метод судової експертизи даних, що визначає значне покращення (або погіршення) результатів, яке може свідчити про шахрайство.

Оцінювання з високими ставками – тести та інші форми оцінки, результати яких мають істотні наслідки для окремої особи або організації.

Перевірка особистих даних – процес розгляду інформації про людини з метою визначення її кваліфікації для складання тесту.

Перерахунок – процес перерахунку результатів після видалення скомпрометованих питань.

Перерва – час для відпочинку між частинами тривалого тесту.

Питання типу "троянський кінь" – навмисно неправильні питання, вбудовані в тест, які допомагають виявити спробу шахрайства або крадіжки тесту.

Підробка бланку відповідей – одна із форм шахрайства, коли неправильні відповіді на папері стираються і замінюються правильними.

Підставний учасник тесту – людина, яка проходить тести за інших.

План безпеки – документ, що описує політику забезпечення безпеки і процедури її організації.

Повторне складання - перездача тесту.

Повторне тестування – процес повторної здачі тесту.

Подібність відповідей – метод судової експертизи даних, який порівнює відповіді кількох осіб, там допомагає виявити спробу шахрайства, списування та проходження тесту підставним учасником.

Попередні результати – неофіційна оцінка, надана учаснику після завершення тестування, яка підлягає подальшому розгляду комітетом безпеки.

Порушена тестова форма – альтернативна форма тестування, яка застосовується для заміни скомпрометованої тестової форми.

Порушення – успішна атака відомих чи невідомих загроз.

Резерв питань – великий набір запитань, з якого обирають пункти для окремого тесту напередодні чи під час тестування.

Ризик – ймовірність виникнення успішної загрози, що призведе до порушення та шкоди.

Розголошення питань – розголошення окремих запитань тесту під час його проведення або після завершення шляхом незаконного збору і поширення через інтернет чи будь-яким іншим способом.

Розпізнавання обличчя – біометричний метод з використанням веб-камер, де риси обличчя людини порівнюються в момент реєстрації і безпосередньо перед проходженням тесту.

Розслідування – процес виявлення причин і масштабів порушення. Розслідування може включати інтерв'ю, судову експертизу даних, аналіз процедур, розгляду звітів тощо.

Спостерігач – особа, яка відповідає за безпеку тесту під час адміністрування тестування. Також згадується як Інспектор.

Стирання – відповіді на паперовому бланку, які були стерті.

Судова експертиза даних – метод аналізу результатів тесту для виявлення випадків шахрайства або крадіжки тесту.

Тренування – форма узгоджених дій, за допомогою яких одна людина допомагає іншій відповідати на запитання під час тестування.

Учасник тесту – людина, що проходить тестування. Також згадується як Випробуваний.

Шахрайство – будь-який вид поведінки, спрямований на покращення результату тестування.

Посилання

Foster, D. F. & Miller, H. L., Jr. (2012). Global Test Security Issues and Ethical Challenges. In A.Ferrero, Y. Korkut, M. M. Leach, G. Lindsay, & M. J. Stevens (Eds.). The Oxford Handbook of International Psychological Ethics (pp. 216-232). Oxford: Oxford University Press.